517.060

Rec'd PCT/PTO 06 DEC 2004

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年12 月18 日 (18.12.2003)

PCT

(10) 国際公開番号
WO 03/105400 A1

(51) 国際特許分類[7]: H04L 9/32

(21) 国際出願番号: PCT/JP03/06585

(22) 国際出願日: 2003 年5 月27 日 (27.05.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-167148 2002 年6 月7 日 (07.06.2002) JP
特願2002-167260 2002 年6 月7 日 (07.06.2002) JP
特願2002-167358 2002 年6 月7 日 (07.06.2002) JP

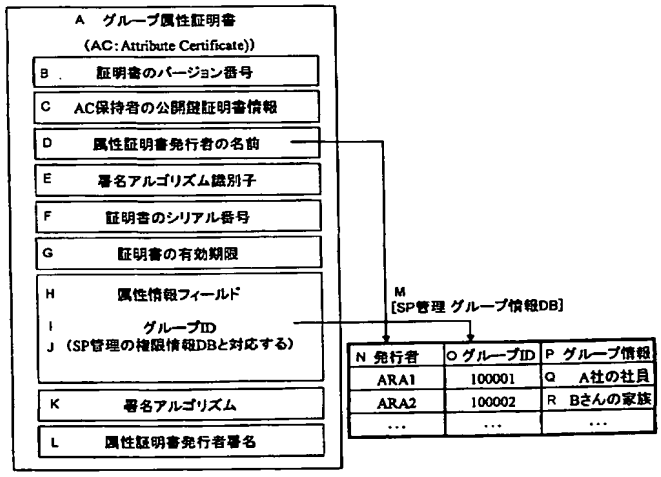
(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 間杉 円 (MASUGI,Madoka) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 島田 昇 (SHIMADA,Noboru) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号

[続葉有]

(54) Title: DATA PROCESSING SYSTEM, DATA PROCESSING DEVICE, DATA PROCESSING METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: データ処理システム、データ処理装置、および方法、並びにコンピュータ・プログラム



A...GROUP ATTRIBUTE CERTIFICATE
B...CERTIFICATE VERSION NUMBER
C...AC HOLDER PUBLIC KEY CERTIFICATE INFORMATION
D...ATTRIBUTE CERTIFICATE ISSUER NAME
E...SIGNATURE ALGORITHM IDENTIFIER
F...CERTIFICATE SERIAL NUMBER
G...CERTIFICATE EXPIRATION DATE
H...ATTRIBUTE INFORMATION FIELD
I...GROUP ID
J...(CORRESPONDING TO THE RIGHT INFORMATION DB OF SP MANAGEMENT)
K...SIGNATURE ALGORITHM
L...ATTRIBUTE CERTIFICATE ISSUER SIGNATURE
M...[SP MANAGEMENT GROUP INFORMATION DB]
N...ISSUER
O...GROUP ID
P...GROUP INFORMATION
Q...STAFFS OF COMPANY A
R...FAMILY OF MR./MS. B

(57) Abstract: A right management system capable of effectively performing right management such as a service reception right check processing. Group identification information which is set corresponding to a group consisting of particular devices or particular users is made to be information to be stored, and a group attribute certificate added by a digital signature of an issuer is issued to a service reception entity. When providing a service, a signature of the group attribute certificate presented is checked to judge whether or not the certificate has been altered and the group identification information stored in the group attribute certificate is examined to judge whether or not the group is a service allowed group by using the group information database. Provision of the service is decided according to the examination. Thus, it is possible to perform a unified right check for various user sets or device sets, omitting individual right information management, thereby enabling effective right management.

(57) 要約: サービス受領権限の確認処理等、効率的な権限管理を可能とする権限管理システムを実現する。特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書をサービス受領エンティテイに発行し、サービス提供時に、提示されるグループ属性証明書の署名検証による改竄有無の検証、グループ属性証明書に格納されたグループ識別情報に基づく、サービス許容グループであるか否かの審査をグループ情報データベースを適用して実行し、審査に基づくサービス提供可否の判定を実行する構成とした。様々なユーザ集合あるいは機器集合に対応する一括した権限確認が可能となり、個別の権限情報の管理が省略でき、効

[続葉有]

WO 03/105400 A1

ソニー株式会社内 Tokyo (JP). 岡 誠 (OKA,Makoto) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 川口 貴義 (KAWAGUCHI,Takayoshi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 石橋 義人 (ISHIBASHI,Yoshihito) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 阿部 博 (ABE,Hiroshi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 豊島 信隆 (TOYOSHIMA,Nobutaka) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 宮田 正昭，外(MIYATA,Masaaki et al.); 〒104-0041 東京都 中央区 新富一丁目１番７号 銀座 ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

データ処理システム、データ処理装置、および方法、並びにコンピュータ・プログラム

技術分野

本発明は、データ処理システム、データ処理装置、および方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、例えばコンテンツ利用、あるいはサービス利用処理等において確認が要求されるユーザのサービス受領権限管理を効率的にかつセキュアに実行し、ユーザあるいは機器のアクセス権限確認に基づいてデータ処理を実行するデータ処理システム、データ処理装置、および方法、並びにコンピュータ・プログラムに関する。

背景技術

昨今、インターネット等の通信網、あるいは、ＤＶＤ、ＣＤ、メモリカード等の流通可能な記憶媒体を介した音楽データ、画像データ、ゲームプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）の配信、あるいは端末間のデータ送受信処理を伴う決済等、端末間の通信処理を伴ったサービス提供処理が盛んに実行されている。例えばＰＣ、携帯通信端末、ポータブルデバイス、あるいはメモリカード等の様々なユーザデバイスを有するユーザが、自宅、外出先等においてユーザデバイスをサービスプロバイダのサービス提供デバイスと接続し、デバイス間で情報の交換、あるいはコンテンツ、サービスの受領を行なうことが日常的になりつつある。

具体的なサービス利用例としては、例えば、ＰＣ、携帯端末等を用いて、コンテンツ配信サービスプロバイダにアクセスし、音楽、動画、ゲームプログラム等の様々なコンテンツをダウンロードしたり、あるいは、個人情報、銀行口

座情報、利用可能金額情報等を格納したＩＣチップ内蔵のメモリカード等を用いて、ショッピングに利用したり、振替処理を行なったり、あるいは、駅の改札、バス等において切符の代替手段として用いるなど、様々な利用がなされつつある。

このように通信網あるいは媒体を介したコンテンツあるいはサービス等の流通が盛んになる一方、コンテンツ、あるいはサービスの不正利用、すなわち正当な権限を有しないユーザによるサービス利用の問題が発生しており、正当な利用権限を有するユーザにのみ確実にコンテンツあるいはサービス等の提供を行ない、サービスの不正利用を排除するシステムの構築が望まれている。

例えば、音楽データ、画像データ、ゲームプログラム等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されており、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないようにセキュリティを考慮したシステムが採用されている。

サービスを受領する機器あるいはユーザの利用制限を実現する１つの手法が、暗号化処理である。例えばコンテンツあるいはサービス情報を機器またはユーザに提供する際に、暗号化して提供し、正規の機器またはユーザのみに利用可能な復号鍵を配布し、コンテンツあるいはサービス利用を可能とする形態がある。暗号化データは、復号鍵を用いた復号化処理によって復号データ（平文）に戻すことができる。

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Data encryption standard）がある。

また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なる鍵で行なう方式がいわゆる公開鍵暗号方式

と呼ばれる方式である。公開鍵暗号方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が生成した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号化処理が可能となる。秘密鍵は、公開鍵を生成した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号方式の代表的なものには、楕円曲線暗号、あるいはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

上記のようなコンテンツあるいはサービスの利用管理構成において、正当なユーザであるか否かの判定は、例えばコンテンツあるいはサービスの提供者であるサービスプロバイダとＰＣ、携帯端末、メモリカード等のユーザデバイス間において、コンテンツ、サービス情報等の暗号化データ、あるいは復号鍵の提供前の認証処理によって行なう方法が知られている。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてコンテンツ、あるいは復号鍵等のデータを暗号化して通信を行なう。

発明の開示

ユーザ権限を確認するシステムとしては、上述のように、サービスを提供するサービスプロバイダとユーザ間で１対１の認証処理を実行し、ユーザ権限の確認を実行する手法があるが、コンテンツ提供サービス、その他の情報利用サービス、決済サービス等、ユーザ端末で実行可能なサービスが多様化するにつれ、個々のユーザ、あるいはユーザ端末のサービス利用権限の有無を効率的に確実にかつセキュアに実行するシステムの構築が望まれている。

本発明は、上記問題点に鑑みてなされたものであり、相互に通信可能な複数

デバイス間において、データ通信を伴ったデータ処理を実行するデータ処理システムにおいて、各デバイスが、通信相手のデバイスあるいはユーザが正当なデータ処理の実行権限、あるいはサービスの受領権限を有するか否かをセキュアにかつ確実に判定して、誤りの無いデータ処理を実現することを可能としたデータ処理システム、データ処理装置、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

例えば、アクセス先となる通信処理装置において認めたユーザあるいは通信機器からのアクセスであるか否かを属性証明書に基づいて審査し、アクセス権限を有するユーザまたは機器からのアクセスのみを許可し、その他の機器からのアクセスを排除する構成を実現する装置、および方法を提供することを目的とする。

本発明の第１の側面は、

ユーザデバイスのサービス受領権限を管理する権限管理システムであり、

サービス受領エンティティとしてのユーザデバイスは、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書を有し、

サービス提供エンティティとしてのサービスプロバイダは、

前記ユーザデバイスから提示されるグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行する構成を有することを特徴とする権限管理システムにある。

さらに、本発明の権限管理システムの一実施態様において、前記グループ属性証明書は、グループ属性証明書発行エンティティとユーザデバイス間における相互認証の成立、および、発行対象としての機器またはユーザが前記サービスプロバイダにより許容された発行ポリシーに従っていることを条件として、機器またはユーザに対応するユーザデバイスに対して発行する証明書である

ことを特徴とする。

さらに、本発明の権限管理システムの一実施態様において、新たなグループ属性証明書の発行処理は、グループ属性証明書発行エンティティにおいて、ユーザデバイスが既に有する既発行のグループ属性証明書についての検証成立を条件として行なう構成であることを特徴とする。

さらに、本発明の権限管理システムの一実施態様において、前記サービスプロバイダは、前記グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを有し、前記ユーザデバイスから提示されるグループ属性証明書に格納されたグループ識別情報に基づいて、前記グループ情報データベースを検索して、サービス提供の可否についての判定処理を実行する構成であることを特徴とする。

さらに、本発明の権限管理システムの一実施態様において、前記サービスプロバイダは、前記ユーザデバイスから提示される複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、該審査に基づくサービス提供可否の判定処理を実行する構成を有することを特徴とする。

さらに、本発明の権限管理システムの一実施態様において、前記サービスプロバイダは、前記ユーザデバイスから機器をグループのメンバとしたグループ定義に基づく第１のグループ属性証明書から取得される第１のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行うとともに、ユーザをグループのメンバとしたグループ定義に基づく第２のグループ属性証明書から取得される第２のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行する構成を有することを特徴とする。

さらに、本発明の権限管理システムの一実施態様において、前記ユーザデバイスは、前記サービスプロバイダとの通信を実行する機器としてのエンドエンティティ、および個人識別デバイスとしてのユーザ識別デバイスを含み、前記グループ属性証明書は、前記エンドエンティティおよびユーザ識別デバイス

各々に対して個別に発行され、グループ属性証明書発行エンティティと前記エンドエンティティ、またはユーザ識別デバイスとの相互認証成立を条件とした発行処理がなされる構成であることを特徴とする。

さらに、本発明の権限管理システムの一実施態様において、前記グループ属性証明書は、属性認証局の発行する属性証明書であり、属性証明書中の属性情報フィールドに、グループ識別子を格納した構成であることを特徴とする。

さらに、本発明の権限管理システムの一実施態様において、前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記サービスプロバイダは、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行する構成であることを特徴とする。

さらに、本発明の第２の側面は、

サービス提供処理としてのデータ処理を実行する情報処理装置であり、

サービス提供先デバイスからサービス利用権限確認処理に適用する属性証明書として、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書を受信するデータ受信部と、

前記グループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行するグループ属性証明書検証処理部と、

を有することを特徴とする情報処理装置にある。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを有し、前記グループ属性証明書検証処理部は、前記サービス提供先デバイスから提示されるグループ属性証明書に格納されたグループ識別情報に基づいて、前記グループ情報データベースを検索して、サービス提供の可否についての判定処理を実行する構成であることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記グループ属性証明書検証処理部は、前記ユーザデバイスから提示される複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、該審査に基づくサービス提供可否の判定処理を実行する構成を有することを特徴とする。

さらに、本発明の第３の側面は、

ユーザデバイスのサービス受領権限を管理する権限管理方法であり、

サービス受領エンティテイとしてのユーザデバイスにおける実行ステップとして、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書をサービス提供エンティテイとしてのサービスプロバイダに送信するステップを有し、

前記サービスプロバイダにおける実行ステップとして、

前記ユーザデバイスから提示されるグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行するステップ、

を有することを特徴とする権限管理方法にある。

さらに、本発明の権限管理方法の一実施態様において、前記権限管理方法において、さらに、機器またはユーザに対応するユーザデバイスに対して前記グループ属性証明書を発行するグループ属性証明書発行処理ステップを有し、該グループ属性証明書発行処理ステップは、グループ属性証明書発行エンティテイとユーザデバイス間における相互認証の成立、および、発行対象としての機器またはユーザが前記サービスプロバイダにより許容された発行ポリシーに従っていることを条件として、機器またはユーザに対応するユーザデバイスに対してグループ属性証明書を発行する処理ステップであることを特徴とする。

さらに、本発明の権限管理方法の一実施態様において、前記グループ属性証

明書発行処理ステップは、ユーザデバイスが既に有する既発行のグループ属性証明書についての検証処理ステップを含み、該検証の成立を条件としてグループ属性証明書の発行を行なうことを特徴とする。

さらに、本発明の権限管理方法の一実施態様において、前記サービスプロバイダは、前記グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを有し、前記ユーザデバイスから提示されるグループ属性証明書に格納されたグループ識別情報に基づいて、前記グループ情報データベースを検索して、サービス提供の可否についての判定処理を実行することを特徴とする。

さらに、本発明の権限管理方法の一実施態様において、前記サービスプロバイダは、前記ユーザデバイスから提示される複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を各々実行し、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行することを特徴とする。

さらに、本発明の権限管理方法の一実施態様において、前記サービスプロバイダは、前記ユーザデバイスから機器をグループのメンバとしたグループ定義に基づく第１のグループ属性証明書から取得される第１のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行うとともに、ユーザをグループのメンバとしたグループ定義に基づく第２のグループ属性証明書から取得される第２のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行することを特徴とする。

さらに、本発明の権限管理方法の一実施態様において、前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記サービスプロバイダは、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行することを特徴とする。

さらに、本発明の第４の側面は、

サービス提供処理としてのデータ処理を実行する情報処理装置における情報処理方法であり、

サービス提供先デバイスからサービス利用権限確認処理に適用する属性証明書として、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書を受信する証明書受信ステップと、

前記グループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行するグループ属性証明書検証処理ステップと、

を有することを特徴とする情報処理方法にある。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理装置は、前記グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを有し、前記グループ属性証明書検証処理ステップは、前記サービス提供先デバイスから提示されるグループ属性証明書に格納されたグループ識別情報に基づいて、前記グループ情報データベースを検索して、サービス提供の可否についての判定処理を実行するステップを含むことを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記グループ属性証明書検証処理ステップは、前記ユーザデバイスから提示される複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を各々実行し、全てのグループ識別情報がサービス許容対象であることの判定を条件として基づくサービス提供可の判定処理を実行するステップを含むことを特徴とする。

さらに、本発明の第５の側面は、

ユーザデバイスのサービス受領権限を管理する権限管理処理を実行せしめるコンピュータ・プログラムであって、

サービス提供先デバイスからサービス利用権限確認処理に適用する属性証

明書として、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書を受信するデータ受信ステップと、

前記グループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行するグループ属性証明書検証処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

さらに、本発明の第６の側面は、

通信機能を有する通信機器間におけるアクセス制限を実行するアクセス権限管理システムであり、

アクセス要求元デバイスは、

特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに、発行者の電子署名を有するグループ属性証明書を記憶手段に格納し、

前記アクセス要求元デバイスからのアクセス要求対象となるアクセス要求先デバイスは、

前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とするアクセス権限管理システムにある。

さらに、本発明のアクセス権限管理システムの一実施態様において、前記アクセス要求先デバイスは、前記アクセス要求元デバイスを構成するアクセス実行機器としてのエンドエンティティに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するエンドエンティティであるか否かの審査を行い、該審査に基づいてアクセス可否

の判定を実行する構成を有することを特徴とする。

さらに、本発明のアクセス権限管理システムの一実施態様において、前記アクセス要求先デバイスは、前記アクセス要求元デバイスを構成する個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とする。

さらに、本発明のアクセス権限管理システムの一実施態様において、前記アクセス要求元デバイス、およびアクセス要求先デバイスは、耐タンパ構成を持つセキュリティチップを有し、相互のセキュリティチップ間における相互認証を実行し、相互認証の成立を条件として、前記アクセス要求先デバイスは、前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証、およびアクセス許容グループに属するデバイスであるか否かの審査を実行する構成であることを特徴とする。

さらに、本発明のアクセス権限管理システムの一実施態様において、前記アクセス要求先デバイスは、デバイスからのアクセス許容グループメンバであることを証明するグループ属性証明書の発行要求を受領するとともに、デバイス間の相互認証の成立、および、グループ属性証明書発行要求デバイスが、前記アクセス要求先デバイスの許容する発行ポリシーに従っていることを条件として、機器またはユーザに対応するデバイスに対してアクセス許容グループメンバであることを証明するグループ属性証明書を発行する処理を実行する構成であることを特徴とする。

さらに、本発明のアクセス権限管理システムの一実施態様において、前記アクセス要求先デバイスは、デバイスからのアクセス許容グループメンバであることを証明するグループ属性証明書の発行要求を受領するとともに、デバイス間の相互認証の成立、および、グループ属性証明書発行要求デバイスが既に保有する既発行のグループ属性証明書の検証および審査の成立を条件として、アクセス許容グループメンバであることを証明するグループ属性証明書を発行する処理を実行する構成であることを特徴とする。

さらに、本発明のアクセス権限管理システムの一実施態様において、前記グループ属性証明書は、グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記アクセス要求先デバイスは、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行する構成であることを特徴とする。

さらに、本発明の第７の側面は、

アクセス制限処理を実行する通信処理装置であり、

アクセス要求元デバイスから特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とし、発行者の電子署名を有するグループ属性証明書を受信する受信部と、

前記アクセス要求元デバイスから受信したグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行するグループ属性証明書検証処理機能を実行するアクセス権限判定処理部と、

を有することを特徴とする通信処理装置にある。

さらに、本発明の通信処理装置の一実施態様において、前記アクセス権限判定処理部は、前記アクセス要求元デバイスにおけるアクセス実行機器としてのエンドエンティティに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するエンドエンティティであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とする。

さらに、本発明の通信処理装置の一実施態様において、前記アクセス権限判定処理部は、前記アクセス要求元デバイスにおける個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とする。

さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、前記アクセス要求元デバイスとの相互認証を実行する暗号処理部を有し、前記アクセス権限判定処理部は、相互認証の成立を条件として、前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証、およびアクセス許容グループに属するデバイスであるか否かの審査を実行する構成を有することを特徴とする。

さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、さらに、特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とし、発行者の電子署名を有するグループ属性証明書を生成する属性証明書生成部を有することを特徴とする。

さらに、本発明の通信処理装置の一実施態様において、前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記アクセス権限判定処理部は、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行する構成であることを特徴とする。

さらに、本発明の第８の側面は、

通信機能を有する通信機器間におけるアクセス制限を実行するアクセス権限管理方法であり、

アクセス要求元デバイスにおいて、

特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに、発行者の電子署名を有するグループ属性証明書をアクセス要求対象となるアクセス要求先デバイスに送信するステップと、

前記アクセス要求先デバイスにおいて、

前記アクセス要求元デバイスから提示されるグループ属性証明書を受信するステップと、

該受信グループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスである

か否かの審査を行う審査ステップと、

前記審査ステップの審査結果に基づいてアクセス可否の判定を実行するステップと、

を有することを特徴とするアクセス権限管理方法にある。

さらに、本発明のアクセス権限管理方法の一実施態様において、前記アクセス要求先デバイスは、前記アクセス要求元デバイスにおけるアクセス実行機器としてのエンドエンティティに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するエンドエンティティであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行することを特徴とする。

さらに、本発明のアクセス権限管理方法の一実施態様において、前記アクセス要求先デバイスは、前記アクセス要求元デバイスにおける個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行することを特徴とする。

さらに、本発明のアクセス権限管理方法の一実施態様において、前記アクセス権限管理方法は、さらに、前記アクセス要求元デバイス、およびアクセス要求先デバイスの有する耐タンパ構成を持つセキュリティチップ間における相互認証実行ステップを有し、前記アクセス要求先デバイスは、相互認証の成立を条件として、前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証、およびアクセス許容グループに属するデバイスであるか否かの審査を実行することを特徴とする。

さらに、本発明のアクセス権限管理方法の一実施態様において、前記アクセス権限管理方法は、さらに、前記アクセス要求先デバイスにおいて、デバイスからのアクセス許容グループメンバであることを証明するグループ属性証明書の発行要求を受信するステップと、デバイス間の相互認証の成立、および、グループ属性証明書発行要求デバイスが、前記アクセス要求先デバイスの許容する発行ポリシーに従っていることを条件として、機器またはユーザに対応す

るデバイスに対してグループ属性証明書を発行する処理を実行するステップと、を有することを特徴とする。

さらに、本発明のアクセス権限管理方法の一実施態様において、前記アクセス権限管理方法は、さらに、前記アクセス要求先デバイスにおける実行ステップとして、デバイスからのアクセス許容グループメンバであることを証明するグループ属性証明書の発行要求に応じて、デバイス間の相互認証の成立、および、グループ属性証明書発行要求デバイスが既に保有する既発行のグループ属性証明書の検証および審査の成立を条件として、アクセス許容グループメンバであることを証明するグループ属性証明書を発行する処理を実行するステップを含むことを特徴とする。

さらに、本発明のアクセス権限管理方法の一実施態様において、前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記アクセス要求先デバイスは、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行することを特徴とする。

さらに、本発明の第９の側面は、

アクセス制限処理を実行する通信処理装置における通信管理方法であり、

アクセス要求元デバイスから特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とし、発行者の電子署名を有するグループ属性証明書を受信する受信ステップと、

前記アクセス要求元デバイスから受信したグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を実行するアクセス権限判定処理ステップと、

該アクセス権限判定処理結果に基づいてアクセス可否の決定を実行するアクセス可否決定処理ステップと、

を有することを特徴とする通信管理方法にある。

さらに、本発明の通信管理方法の一実施態様において、前記アクセス権限判

定処理ステップは、前記アクセス要求元デバイスにおけるアクセス実行機器としてのエンドエンティティに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するエンドエンティティであるか否かの審査を行なうステップを含むことを特徴とする。

さらに、本発明の通信管理方法の一実施態様において、前記アクセス権限判定処理ステップは、前記アクセス要求元デバイスにおける個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行なうステップを含むことを特徴とする。

さらに、本発明の通信管理方法の一実施態様において、前記通信管理方法において、さらに、前記アクセス要求元デバイスとの相互認証を実行する認証処理ステップを有し、前記アクセス権限判定処理ステップは、相互認証の成立を条件として、前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証、およびアクセス許容グループに属するデバイスであるか否かの審査を実行することを特徴とする。

さらに、本発明の通信管理方法の一実施態様において、前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、前記アクセス権限判定処理ステップは、前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行することを特徴とする。

さらに、本発明の第１０の側面は、

アクセス制限処理を実行する通信処理装置における通信管理処理を実行せしめるコンピュータ・プログラムであって、

アクセス要求元デバイスから特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とし、発行者の電子署名を有するグループ属性証明書を受信する受信ステップと、

前記アクセス要求元デバイスから受信したグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容

グループに属するデバイスであるか否かの審査を実行するアクセス権限判定処理ステップと、

該アクセス権限判定処理結果に基づいてアクセス可否の決定を実行するアクセス可否決定処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

さらに、本発明の第１１の側面は、

相互に通信可能な複数デバイス間において、データ通信処理を伴うデータ処理を実行するデータ処理システムであり、

前記複数デバイス中、通信相手デバイスに対するデータ処理を要求するデータ処理要求元デバイスは、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を格納し、データ処理要求処理に際して、該グループ属性証明書をデータ処理要求先デバイスに対して送信し、

前記データ処理要求先デバイスは、

受領したグループ属性証明書の検証処理を実行し、該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定し、権限有りの判定に基づいてデータ処理を実行する構成としたことを特徴とするデータ処理システムにある。

さらに、本発明のデータ処理システムの一実施態様において、データ処理要求元デバイスに格納されるグループ属性証明書は、データ処理要求先デバイスが発行者であり、該データ処理要求先デバイスの電子署名を有し、前記データ処理要求先デバイスは、受領したグループ属性証明書の検証処理として、自デバイスの公開鍵を適用した電子署名検証処理を実行する構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、前記相互に通信可能な複数デバイスのいずれもが、通信相手デバイスに対するデータ処理を相互に要求するデバイスであり、通信相手デバイスの発行したグループ属性証

明書を各々格納した構成を有し、各デバイス各々が、通信相手に対するデータ処理要求時に自デバイスに格納したグループ属性証明書を送信し、受領デバイスにおける検証成立を条件として、データ処理要求に応じた処理を相互に実行する構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、前記相互に通信可能な複数デバイス各々は、耐タンパ構成を持つセキュリティチップを有し、通信相手デバイスに対するデータ処理要求に際して、相互のセキュリティチップ間における相互認証を実行し、相互認証の成立を条件として、デバイス間におけるグループ属性証明書の送信、および送信グループ属性証明書の検証を実行する構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、データ処理要求元デバイスに格納されるグループ属性証明書は、データ処理要求先デバイスが発行者であり、データ処理要求元デバイスとデータ処理要求先デバイス間の相互認証の成立を条件として発行処理がなされることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、前記相互に通信可能な複数のデバイス中、少なくとも１以上のデバイスは、デバイス構成として、他デバイスとの通信処理およびデータ処理を実行するエンドエンティティと、該エンドエンティティとデータ送受信可能な個人識別機能を有するユーザ識別デバイスとを有し、前記グループ属性証明書が特定のユーザグループの構成メンバに対して発行される場合、前記ユーザ識別デバイスと、グループ属性証明書発行処理実行デバイス間の相互認証の成立を条件とした発行処理がなされる構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、前記相互に通信可能な複数デバイスの一方は、デバイスに対するメンテナンス処理を実行するメンテナンス実行デバイスであり、他方のデバイスは、前記メンテナンス実行デバイスによるメンテナンスサービスを受領するサービス受領デバイスであり、前記サービス受領デバイスは、前記メンテナンス実行デバイスの発行したグループ属性証明書としてのサービス属性証明書を格納し、前記メンテナンス実行デバイスは、前記サービス受領デバイスの発行したグループ属性証明書

としてのコントロール属性証明書を格納し、前記サービス属性証明書は、前記サービス受領デバイスがメンテナンスサービス受領権限を有する機器またはユーザのグループに属することを前記メンテナンス実行デバイスにおいて検証するために適用され、前記コントロール属性証明書は、前記メンテナンス実行デバイスが、メンテナンスサービス実行権限を有する機器またはユーザのグループに属することを前記サービス受領デバイスにおいて検証するために適用される構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、前記サービス受領デバイスにおいて実行されるメンテナンスプログラムは、暗号化メンテナンスプログラムとして、前記サービス受領デバイスに送信または格納され、前記サービス受領デバイスは、前記暗号化メンテナンスプログラムを耐タンパ構成を有するセキュリティチップ内で復号した後、前記サービス受領デバイスにおいて実行する構成であることを特徴とする。

さらに、本発明のデータ処理システムの一実施態様において、前記サービス受領デバイスにおいて実行されるメンテナンス処理は、前記メンテナンス実行デバイスから前記サービス受領デバイスに対して送信されるコマンドに基づいて実行され、前記サービス受領デバイスは、受信コマンドの実行結果を前記メンテナンス実行デバイスに応答送信し、前記メンテナンス実行デバイスは、該応答送信に基づく新たなコマンド送信を前記サービス受領デバイスに対して実行する構成であることを特徴とする。

さらに、本発明の第１２の側面は、

データ処理要求デバイスからのデータ処理要求に基づくデータ処理を実行するデータ処理装置であり、

前記データ処理要求デバイスから、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を受信するデータ受信部と、

受領したグループ属性証明書の検証処理を実行し、該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定する権限判定処理部と、

権限有りの判定に基づいてデータ処理を実行するデータ処理部と、

を有することを特徴とするデータ処理装置にある。

さらに、本発明のデータ処理装置の一実施態様において、前記権限判定処理部は、受領したグループ属性証明書の検証処理として、自デバイスの公開鍵を適用した電子署名検証処理を実行する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、前記データ処理装置は、耐タンパ構成を持ち暗号処理部を有するセキュリティチップを有し、前記暗号処理部は、データ処理要求デバイスからのデータ処理要求に応じて、データ処理要求デバイスとの相互認証を実行する構成を有し、前記権限判定処理部は、相互認証の成立を条件として、グループ属性証明書の検証を実行する構成であることを特徴とする。

さらに、本発明のデータ処理装置の一実施態様において、前記データ処理装置は、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに電子署名を有するグループ属性証明書を生成する機能を持つ属性証明書生成処理部を有する構成であることを特徴とする。

さらに、本発明の第１３の側面は、

相互に通信可能な複数デバイス間において、データ通信処理を伴うデータ処理を実行するデータ処理方法であり、

前記複数デバイス中、通信相手デバイスに対するデータ処理を要求するデータ処理要求元デバイスにおいて、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を、データ処理要求処理に際して、該グループ属性証明書をデータ処理要求先デバイスに対して送信するステップを実行し、

前記データ処理要求先デバイスは、

受領したグループ属性証明書の検証処理ステップ、

該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定するステップ、

権限有りの判定に基づいてデータ処理を実行するステップ、

を実行することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、データ処理要求元デバイスに格納されるグループ属性証明書は、データ処理要求先デバイスが発行者であり、該データ処理要求先デバイスの電子署名を有し、前記データ処理要求先デバイスにおける前記検証処理ステップは、受領したグループ属性証明書の検証処理として、自デバイスの公開鍵を適用した電子署名検証処理を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、前記相互に通信可能な複数デバイスのいずれもが、通信相手デバイスに対するデータ処理を相互に要求するデバイスであって、通信相手デバイスの発行したグループ属性証明書を各々格納した構成を有し、各デバイスいずれもが、通信相手に対するデータ処理要求時に自デバイスに格納したグループ属性証明書を送信し、受領デバイスにおける検証成立を条件として、データ処理要求に応じた処理を相互に実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、前記相互に通信可能な複数デバイス各々は、耐タンパ構成を持つセキュリティチップを有し、通信相手デバイスに対するデータ処理要求に際して、相互のセキュリティチップ間における相互認証を実行し、相互認証の成立を条件として、デバイス間におけるグループ属性証明書の送信、および送信グループ属性証明書の検証を実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において、さらに、データ処理要求元デバイスに格納されるグループ属性証明書の発行処理ステップを有し、該発行処理ステップは、データ処理要求元デバイスとデータ処理要求先デバイス間の相互認証の成立を条件として実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において、さらに、データ処理要求元デバイスに格納されるグループ属性証明書の発行処理ステップを有し、該発行処理ステップは、前記グループ属性証

明書を特定のユーザグループの構成メンバに対して発行する場合、データ処理要求元デバイスを構成する個人識別機能を有するユーザ識別デバイスとの相互認証の成立を条件とした発行処理を行なうことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、前記相互に通信可能な複数デバイスの一方は、デバイスに対するメンテナンス処理を実行するメンテナンス実行デバイスであり、他方のデバイスは、前記メンテナンス実行デバイスによるメンテナンスサービスを受領するサービス受領デバイスであり、前記サービス受領デバイスにおける、前記メンテナンス実行デバイスの発行したグループ属性証明書としてのサービス属性証明書を前記メンテナンス実行デバイスに送信するステップと、前記メンテナンス実行デバイスにおける、受信サービス属性証明書の検証を実行するサービス属性証明書検証ステップと、前記メンテナンス実行デバイスにおける、前記サービス受領デバイスの発行したグループ属性証明書としてのコントロール属性証明書を前記サービス受領デバイスに送信するステップと、前記サービス受領デバイスにおける、受信コントロール属性証明書の検証を実行するコントロール属性証明書検証ステップと、前記サービス属性証明書検証、およびコントロール属性証明書検証の両検証が成立したことを条件としてメンテナンス処理を実行するメンテナンス処理ステップと、を有することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、前記サービス受領デバイスにおいて実行されるメンテナンス処理プログラムは、暗号化メンテナンスプログラムとして、前記サービス受領デバイスに送信または格納され、前記サービス受領デバイスは、前記暗号化メンテナンスプログラムを耐タンパ構成を有するセキュリティチップ内で復号した後、前記サービス受領デバイスにおいて実行することを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、前記サービス受領デバイスにおいて実行されるメンテナンス処理は、前記メンテナンス実行デバイスから前記サービス受領デバイスに対して送信されるコマンドに基づいて実行され、前記サービス受領デバイスは、受信コマンドの実行結果を前記メンテナンス実行デバイスに応答送信し、前記メンテナンス実行デバイスは、該応

答送信に基づく新たなコマンド送信を前記サービス受領デバイスに対して実行することを特徴とする。

さらに、本発明の第１４の側面は、

データ処理要求デバイスからのデータ処理要求に基づくデータ処理を実行するデータ処理方法であり、

前記データ処理要求デバイスから、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を受信するデータ受信ステップと、

受信したグループ属性証明書の検証処理を実行し、該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定する権限判定処理ステップと、

権限有りの判定に基づいてデータ処理を実行するデータ処理ステップと、

を有することを特徴とするデータ処理方法にある。

さらに、本発明のデータ処理方法の一実施態様において、前記権限判定処理ステップは、受領したグループ属性証明書の検証処理として、自デバイスの公開鍵を適用した電子署名検証処理を実行するステップを含むことを特徴とする。

さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において、さらに、データ処理要求デバイスからのデータ処理要求に応じて、データ処理要求デバイスとの相互認証を実行するステップを有し、前記権限判定処理ステップは、相互認証の成立を条件として、グループ属性証明書の検証を実行することを特徴とする。

さらに、本発明の第１５の側面は、

データ処理要求デバイスからのデータ処理要求に基づくデータ処理を実行せしめるコンピュータ・プログラムであって、

前記データ処理要求デバイスから、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を受信するデータ受信ステッ

プと、

受領したグループ属性証明書の検証処理を実行し、該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定する権限判定処理ステップと、

権限有りの判定に基づいてデータ処理を実行するデータ処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

本発明の構成によれば、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書をサービス受領エンティテイに発行し、サービス提供時に、提示されるグループ属性証明書の署名検証による改竄有無の検証、グループ属性証明書に格納されたグループ識別情報に基づく、サービス許容グループであるか否かの審査を実行し、審査に基づくサービス提供可否の判定を実行する構成としたので、様々なユーザ集合あるいは機器集合に対応する一括した権限確認が可能となり、個別の権限情報の管理が省略可能となり、効率的な権限管理が可能となる。

さらに、本発明の構成によれば、グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを適用してサービス提供の可否についての判定が可能となり、グループ毎の設定権限の詳細な区別が可能となる。

さらに、本発明の構成によれば、複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を各々実行し、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行することが可能であり、機器に対応して設定されたグループおよびユーザに対して設定されたグループ等の重複条件に基づくサービスの提供等、様々な態様での権限設定が可能となる。

さらに、本発明の構成によれば、特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとと

もに、発行者の電子署名を有するグループ属性証明書に格納されたグループ識別情報に基づいて、アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を行い、審査に基づいてアクセス可否の判定を実行する構成としたので、通信処理装置を有するユーザが任意に設定したグループのメンバとしてのユーザまたはユーザ機器としてのアクセス要求元の通信処理装置グループのみにアクセスを許可することが可能となる。

さらに、本発明の構成によれば、アクセス要求元デバイスを構成する個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、アクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行い、アクセス可否の判定を実行する構成としたので、通信処理装置を変更した場合であっても、個人識別デバイスとしてのユーザ識別デバイスに対して発行したグループ属性証明書に基づく審査においてアクセスを許可することが可能となり、通信処理装置の変更によってアクセスが拒否されてしまうといったことを防止できる。

さらに、本発明の構成によれば、通信相手デバイスに対するデータ処理を要求するデータ処理要求元デバイスが、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報としたグループ属性証明書をデータ処理要求先デバイスに対して送信して、データ処理要求先デバイスにおいて、グループ属性証明書の検証処理を実行して、検証に基づいてデータ処理要求元デバイスのデータ処理要求権限の有無を判定し、権限有りの判定に基づいてデータ処理を実行する構成としたので、誤った機器あるいはユーザによる処理が実行されることが防止され、正当な権限に基づく正しいデータ処理が実行されることになる。

さらに、本発明の構成によれば、複数のデータ処理装置のそれぞれが通信相手デバイスに対して相互にデータ処理を要求し、協業したデータ処理を実行する構成においても、各デバイス各々が、通信相手に対するデータ処理要求時に自デバイスに格納したグループ属性証明書を送信し、受領デバイスにおける検証成立を条件として、データ処理要求に応じた処理を相互に実行することにより、複数のデータ処理装置における通信を伴う協業したデータ処理を正しく実

行することが可能となる。

さらに、本発明の構成によれば、メンテナンス実行デバイスと、メンテナンスサービス受領デバイスとにそれぞれコントロール属性証明書、サービス属性証明書を格納し、メンテナンスサービス実行時にそれぞれの属性証明書を交換して、各デバイスにおいて相互に検証、審査して、審査成立を条件としたメンテナンス処理を実行する構成としたので、それぞれの設定した権限範囲で、確実なメンテナンス処理を実現することが可能となる。

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

図１は、権限管理システムにおける公開鍵基盤、権限管理基盤構成について説明する図である。

図２は、公開鍵証明書のフォーマットを示す図である。

図３は、公開鍵証明書のフォーマットを示す図である。

図４は、公開鍵証明書のフォーマットを示す図である。

図５は、権限情報証明書としての属性証明書のフォーマットを示す図である。

図６は、グループ属性証明書（グループＡＣ）の発行者、所有者、検証者、

属性情報の構成例を示す図である。

図７は、グループ属性証明書の発行ポリシーテーブルを示す図である。

図８は、権限管理システムに参加する各エンティティの信頼関係構成を説明するトラストモデルを示す図である。

図９は、ユーザデバイスとしてのエンドエンティティ（ＥＥ）とユーザ識別デバイス（ＵＩＤ）に構成されるセキュリティチップの構成例を示す図である。

図１０は、ユーザデバイスのセキュリティチップの格納データ例を示す図である。

図１１は、グループ属性証明書の発行申請、発行処理、利用処理の流れの概略を説明する図である。

図１２は、サービスプロバイダ（ＳＰ）と、属性認証局（ＡＡ）または属性証明書登録局（ＡＲＡ）のグループ情報共有化処理について説明する図である。

図１３は、公開鍵暗号方式の１つの認証処理方式であるハンドシェイクプロトコル（ＴＬＳ１．０）について示す図である。

図１４は、メッセージ認証コード：ＭＡＣ（Message Authentication Code）の生成構成を示す図である。

図１５は、発行ポリシーテーブル、グループ情報データベースの情報構成例を示す図である。

図１６は、ユーザデバイスであるエンドエンティティ（ＥＥ）のセキュリティチップ（ＳＣ）がグループ属性証明書の発行要求主体である場合の処理シーケンスを示す図である。

図１７は、電子署名の生成処理を説明するフロー図である。

図１８は、電子署名の検証処理を説明するフロー図である。

図１９は、ユーザ識別デバイス（ＵＩＤ）内のユーザセキュリティチップ（ＵＳＣ）対応のグループ属性証明書を発行する手順について説明するシーケンス図である。

図２０は、グループ属性証明書を利用したサービス利用権限確認を含むサービス開始までの処理について説明するシーケンス図である。

図２１は、公開鍵証明書（ＰＫＣ）と属性証明書（ＡＣ）との関連について

説明する図である。

図２２は、属性証明書（ＡＣ）の検証処理フローを示す図である。

図２３は、公開鍵証明書（ＰＫＣ）の検証処理フローを示す図である。

図２４は、グループ属性証明書を利用したサービス利用権限確認を含むサービス開始までの処理について説明するシーケンス図である。

図２５は、グループ属性証明書（Ｇｐ．ＡＣ）の審査処理を説明するシーケンス図である。

図２６は、サービスを提供条件として、ユーザあるいはユーザ機器が異なる複数のグループに属することが条件とされる場合の概念を説明する図である。

図２７は、ユーザ識別デバイス（ＵＩＤ）内のユーザセキュリティチップ（ＵＳＣ）に対応して発行されたグループ属性証明書に基づくサービス提供までの処理について説明するシーケンス図である。

図２８は、ユーザ識別デバイス（ＵＩＤ）内のユーザセキュリティチップ（ＵＳＣ）に対応して発行されたグループ属性証明書に基づくサービス提供までの処理について説明するシーケンス図である。

図２９は、ユーザデバイス間においてグループ属性証明書を発行し、格納する処理について説明するシーケンス図である。

図３０は、アクセス許可情報を属性として持つグループ属性証明書の発行処理シーケンスについて説明する図である。

図３１は、アクセス許可情報をグループ情報として持つグループ属性証明書と、他のグループ属性証明書との対応例について説明する図である。

図３２は、アクセス要求先ユーザデバイスが、自ら属性証明書の発行処理を実行せずに属性証明書の発行処理を他のユーザデバイスに依頼して実行する処理シーケンスについて説明する図である。

図３３は、アクセス許可情報をグループ情報として定義したグループ属性証明書を利用したアクセス可否判定処理を伴うサービス利用シーケンスについて説明する図である。

図３４は、各サービスにおいて利用されるグループ属性証明書の例を示す図である。

図３５は、第１のグループ属性証明書Ａに基づいて、コンテンツの利用許可情報をグループ情報として含む第２のグループ属性証明書Ｂを発行する処理について説明するシーケンス図である。

図３６は、グループ属性証明書Ｂをサービスプロバイダに提示して、コンテンツ利用権限のあることの確認を行なって、サービス提供、すなわちコンテンツ配信サービスを受領する処理について説明するシーケンス図である。

図３７は、複数の異なる属性証明書を適用してユーザあるいはユーザ機器のコンテンツ利用権を確認してサービスを提供する処理に適用する属性証明書例を説明する図である。

図３８は、異なるグループ属性証明書を適用したコンテンツ利用権限確認および、サービス提供処理について説明するフロー図である。

図３９は、サービス提供条件として設定されるグループ属性証明書の組み合わせテーブルデータ構成例を示す図である。

図４０は、複数のグループ属性証明書を適用した利用権限確認処理を説明する図である。

図４１は、医療処理において適用するグループ属性証明書の例を示す図である。

図４２は、医療処理を行なうリモートコントロールのシステムにおいて、各機器に格納される属性証明書について説明する図である。

図４３は、ユーザ識別デバイスに格納されたグループ属性証明書を適用して医療診断プログラムの実行サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する図である。

図４４は、グループ属性証明書を適用して医療診断プログラムの実行結果としての診断データ引き取り処理サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する図である。

図４５は、リモートメンテナンス処理において適用するグループ属性証明書の例を示す図である。

図４６は、メンテナンスサービスを行なうシステムにおいて、各機器に格納される属性証明書を説明する図である。

図４７は、サービス実行時におけるサービス属性証明書およびコントロール属性証明書の利用形態について説明する図である。

図４８は、家電機器（ＥＥ）に格納されたサービス属性証明書、サービスプロバイダに格納されたコントロール属性証明書を適用したメンテナンス等のサービス処理を説明するシーケンス図である。

図４９は、サービス属性証明書の審査処理について説明する図である。

図５０は、コントロール属性証明書に基づくサービス、例えば家電機器に対するメンテナンス処理を実行するシーケンスについて説明する図である。

図５１は、メンテナンス実行プログラムをメーカー側機器（ＳＰ）からユーザ側家電機器（ＥＥ）に対して送信する処理とした例を説明する図である。

図５２は、メンテナンス実行プログラムをメーカー側機器（ＳＰ）から、逐次コマンドを家電機器（ＥＥ）に送信し、コマンド実行に基づく応答を家電機器（ＥＥ）から受信しながらレスポンス対応の処理を実行する例を説明する図である。

図５３は、サービス提供要求時にサービス属性証明書、コントロール属性証明書をメーカー側（ＳＰ）に提示する処理例を説明する図である。

図５４は、コミュニケーションサービスにおいて適用するグループ属性証明書の例を説明する図である。

図５５は、コミュニケーションサービスにおいて適用するグループ属性証明書の格納構成例を示す図である。

図５６は、グループ属性証明書を適用してチャットルーム参加サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する図である。

図５７は、グループ属性証明書を適用してアクセス権限確認処理を行ない、コミュニケーションを開始する処理シーケンスについて説明する図である。

図５８は、実行属性証明書の概要について説明する図である。

図５９は、実行属性証明書の利用手続き概要を説明するフロー図である。

図６０は、実行属性証明書の発行シーケンス図である。

図６１は、実行属性証明書の発行シーケンス図である。

図６２は、実行ＡＣテーブルの構成例を示す図である。

図６３は、セキュリティモジュール（ＳＭ）における登録鍵生成実行ＡＣの生成処理を説明する図である。

図６４は、セキュリティチップで実行される登録鍵生成実行ＡＣに基づく登録鍵生成処理について、説明する図である。

図６５は、セキュリティモジュール（ＳＭ）によるサービス提供実行ＡＣの生成処理を説明する図である。

図６６は、サービス提供実行ＡＣのユーザデバイス側における適用シーケンスをまとめた図である。

図６７は、セキュリティチップ（ＳＣ）におけるサービス提供処理における処理詳細を説明する図である。

図６８は、セキュリティチップ（ＳＣ）登録鍵破棄処理について説明する図である。

図６９は、リセット要求に基づく登録鍵の破棄処理としてのリセット処理を説明する図である。

図７０は、実行属性証明書をサービスプロバイダ（ＳＰ）の承認の下に破棄し、破棄が間違いなく実行されたことをサービスプロバイダに通知する実行属性証明書リセット（破棄）処理について説明する図である。

図７１は、実行属性証明書をサービスプロバイダ（ＳＰ）の承認の下に破棄し、破棄が間違いなく実行されたことをサービスプロバイダに通知する実行属性証明書リセット（破棄）処理について説明する図である。

図７２は、リセット確認結果生成処理の詳細について説明する図である。

図７３は、実行ＡＣに基づく登録鍵の破棄処理について説明する図である。

図７４は、回数制限付きサービス提供実行属性証明書をユーザデバイスにおいて適用してサービスを適用する処理を説明する図である。

図７５は、回数制限付きサービス提供実行属性証明書をユーザデバイスにおいて適用してサービスを適用する処理を説明する図である。

図７６は、更新後の残利用回数≧１の場合のセキュリティチップ（ＳＣ）における処理を説明する図である。

図７７は、更新後の残利用回数＝０の場合のセキュリティチップ（ＳＣ）における処理を説明する図である。

図７８は、譲渡機能付きサービス提供実行属性証明書の適用処理を説明する図である。

図７９は、譲渡機能付きサービス提供実行属性証明書の復号処理以降の処理詳細を説明する図である。

図８０は、譲渡機能付きサービス提供実行属性証明書の復号処理以降の処理詳細を説明する図である。

図８１は、譲渡機能付きサービス提供実行属性証明書を適用した暗号化データ復号処理を説明する図である。

図８２は、審査代行実行属性証明書の概要を説明する図である。

図８３は、審査代行実行属性証明書を適用した処理を説明する図である。

図８４は、審査代行グループ属性証明書を生成、発行する処理について説明する図である。

図８５は、審査代行実行属性証明書を入力して審査代行グループ属性証明書を生成する処理を説明する図である。

図８６は、代理署名実行属性証明書の概要を説明する図である。

図８７は、代理署名実行属性証明書を適用した処理を説明する図である。

図８８は、サービスプロバイダ（ＳＰ）等の検証者からの代理署名グループ属性証明書の提示要求に際して実行する処理を説明する図である。

図８９は、ユーザデバイス、サービスプロバイダ等、各エンティテイの情報処理装置構成例を示す図である。

発明を実施するための最良の形態

以下、本発明について図面を参照して詳細に説明する。なお、以下、下記に示す項目順に説明する。

（１）権限管理システム構成概要

（２）ユーザデバイス構成
（３）グループ属性証明書発行、利用処理
（３－１）グループ属性証明書発行前準備処理
（３－２）グループ属性証明書発行処理
（３－３）グループ属性証明書利用処理
（４）ユーザデバイス間におけるグループ属性証明書の発行、利用処理
（５）グループ属性証明書の具体的利用例
（５－１）コンテンツ配信サービス
（５－２）リモートコントロールサービス
（５－３）リモートメンテナンスサービス
（５－４）パーソナルコミュニュケーションサービス
（６）実行属性証明書（実行ＡＣ）
（６－１）実行属性証明書概要
（６－２）実行属性証明書発行処理
（６－３）実行属性証明書適用処理
（６－４）登録鍵リセット処理
（６－５）実行属性証明書リセット（破棄）処理
（７）実行属性証明書の具体的利用処理
（７－１）回数制限付きサービス提供実行属性証明書
（７－２）譲渡機能付きサービス提供実行属性証明書
（７－３）代理発行実行属性証明書
（８）各エンティティの構成

［（１）権限管理システム概要］

本発明の権限管理システムは、図１に示すように、公開鍵証明書（ＰＫＣ：Ｐｕｂｌｉｃ Ｋｅｙ ｃｅｒｔｉｆｉｃａｔｅ）１２１に基づく公開鍵基盤（ＰＫＩ：Ｐｕｂｌｉｃ Ｋｅｙ ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）１０１、属性証明書（ＡＣ：Ａｔｔｒｉｂｕｔｅ ｃｅｒｔｉｆｉｃａｔｅ）１２２に基づく権限管理基盤（ＰＭＩ：Ｐｒｉｖｉｌｅｇｅ ｍａｎａｇｅｍｅｎｔ Ｉｎ

ｆｒａｓｔｒｕｃｔｕｒｅ）１０２を基本インフラとし、これらのインフラの下で、耐タンパ性のセキュリティチップ（あるいはセキュリティモジュール）を持つユーザデバイス１１１、１１３およびサービスプロバイダ側のサービスプロバイダデバイス１１２間、あるいはユーザデバイス１１１、１１３相互間において権限確認処理を実行するとともに、権限確認に基づくサービス提供処理を実行する構成を持つ。

ユーザデバイス１１１，１１３は、例えば、サービスプロバイダ１１２から音楽、画像、プログラム等の各種コンテンツ提供サービス、その他の情報利用サービス、決済サービス等の各種サービスの提供を受領するユーザの端末であり、具体的には、ＰＣ、ゲーム端末、ＤＶＤ，ＣＤ等の再生装置、携帯通信端末、ＰＤＡ、メモリカード等である。

また、ユーザデバイス１１１，１１３は、ユーザデバイス相互間における通信処理が実行可能な端末であり、各ユーザデバイスに対するアクセス可否等の処理を権限確認に基づいて実行する。ユーザデバイスは、耐タンパ構成のセキュリティチップを搭載している。ユーザデバイスの詳細については後述する。

サービスプロバイダ１１２は、セキュリティチップを持つユーザデバイス１１１，１１３に対してコンテンツ提供、決済処理等の各種サービス提供を行なうサービスプロバイダである。図１には、ユーザデバイスを２つとサービスプロバイダを１つのみ示してあるが、公開鍵基盤（ＰＫＩ）１０１、権限管理基盤（ＰＭＩ）１０２のインフラの下には、多数のユーザデバイスおよびサービスプロバイダが存在し、それぞれが権限確認に基づくサービス提供を実行する。なお、サービスは、サービスプロバイダがユーザデバイスに対して提供するのみならず、ユーザデバイス間においても相互にサービスの提供が行なわれる。

（公開鍵証明書：ＰＫＣ）

次に、公開鍵基盤について説明する。公開鍵基盤（ＰＫＩ：Ｐｕｂｌｉｃ Ｋｅｙ ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）１０１は、公開鍵証明書（ＰＫＣ：Ｐｕｂｌｉｃ Ｋｅｙ ｃｅｒｔｉｆｉｃａｔｅ）を適用して通信エンティテイ間の認証処理、あるいは転送データの暗号処理等を実行可能とした基盤（インフラ）である。（公開鍵証明書（ＰＫＣ））について図２，図３、図４を用いて説

明する。公開鍵証明書は、認証局（ＣＡ：Certification Authority）が発行する証明書であり、ユーザ、各エンティテイが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

なお、認証局（ＣＡ）の事務代理機関として、登録局（ＲＡ：Registration Authority）を設け、登録局（ＲＡ）において、公開鍵証明書（ＰＫＣ）の発行申請受理、申請者の審査、管理を行なう構成が一般的となっている。

公開鍵証明書のフォーマット例を図２～図４に示す。これは、公開鍵証明書フォーマットＩＴＵ－Ｔ　Ｘ．５０９に準拠した例である。

バージョン（version）は、証明書フォーマットのバージョンを示す。

シリアルナンバ（Serial Number）は、公開鍵証明書の認証局（ＣＡ）によって設定される公開鍵証明書のシリアルナンバである。

シグネチャ（Signature）は、証明書の署名アルゴリズムである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。

発行者（issuer）は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局（ＩＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト公開鍵情報(subject Public Key Info)は、証明書所有者の公開鍵情報として鍵のアルゴリズム、鍵が格納される。

証明局鍵識別子（authority Key Identifier－key Identifier、authority Cert Issuer、authority Cert Serial Number）は、署名検証に用いる証明書発行者の鍵を識別する情報であり、鍵識別子、機関証明書発行者の名称、機関証明書シリアル番号を格納する。

サブジェクト鍵識別子（subject key Identifier）は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を格納する。

鍵使用目的（key usage）は、鍵の使用目的を指定するフィールドであり、（０）ディジタル署名用、（１）否認防止用、（２）鍵の暗号化用、（３）メッセージの暗号化用、（４）共通鍵配送用、（５）認証の署名確認用、（６）失効リストの署名確認用の各使用目的が設定される。

秘密鍵有効期限(private Key Usage Period)は、証明書に格納した公開鍵に対応する秘密鍵の有効期限を記録する。

認証局ポリシー（certificate Policies）は、公開鍵証明書発行者の証明書発行ポリシーを記録する。例えばＩＳＯ／ＩＥＣ９３８４－１に準拠したポリシーＩＤ、認証基準である。

ポリシー・マッピング（policy Mapping）は、認証パス中のポリシー関係の制限に関する情報を格納するフィールドであり、認証局（ＣＡ）証明書にのみ必要となる。

サブジェクト別名（subject Alt Name）は、証明書所有者の別名を記録するフィールドである。

発行者別名（issuer Alt Name）は、証明書発行者の別名を記録するフィールドである。

サブジェクト・ディレクトリ・アトリビュート（subject Directory Attribute）は、証明書所有者のために必要とされるディレクトリの属性を記録するフィールドである。

基本制約（basic Constraint）は、証明対象の公開鍵が認証局（ＣＡ）の署名用か、証明書所有者のものかを区別するためのフィールドである。

許容サブツリー制約名（name Constraints permitted Subtrees）は、発行者が発行する証明書の名前の制限情報を格納するフィールドである。

制約ポリシー（policy Constraints）は、認証パス中のポリシーの関係の制限情報を格納するフィールドである。

ＣＲＬ参照ポイント（Certificate Revocation List Distribution Points）は、証明書所有者が証明書を利用する際に、証明書が失効していないか、どうかを確認するための失効リストの参照ポイントを記述するフィールドである。

署名アルゴリズム（Signature Algorithm）は、証明書の署名付けに用いる

アルゴリズムを格納するフィールドである。

署名は、公開鍵証明書発行者の署名フィールドである。電子署名は、証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行者の秘密鍵を用いて生成したデータである。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

認証局は、図２～図４に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための失効リスト(Revocation List)の作成、管理、配布(これをリボケーション:Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

（属性証明書：ＡＣ）

権限管理基盤（ＰＭＩ：Ｐｒｉｖｉｌｅｇｅ ｍａｎａｇｅｍｅｎｔ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）１０２は、属性証明書（ＡＣ：Ａｔｔｒｉｂｕｔｅ ｃｅｒｔｉｆｉｃａｔｅ）１２２を適用した権限確認処理を実行可能とする基盤（インフラ）である。属性証明書の１形態としてのグループ属性証明書（グループＡＣ)について図５乃至図７を参照して説明する。属性証明書の機能は、サービス利用権限の確認機能であり、属性証明書には、例えばサービスプロバイダの提供するコンテンツ、あるいはサービスの利用権といった権利関連情報や権限に関する所有者の属性情報が記述される。

属性証明書は、基本的には属性認証局（ＡＡ：Attribute Authority）が発行する証明書であり、証明書発行対象の属性情報を格納し、属性認証局側がＩＤや有効期限等の情報を付加し、さらに属性認証局の秘密鍵による署名を付加して作成される証明書である。ただし、以下において説明するグループ属性証明書、実行属性証明書は、必ずしも属性認証局（ＡＡ：Attribute Authority)

が発行機関として限定されるものではなく、サービスプロバイダ、ユーザデバイスにおける発行処理が可能である。

なお、属性認証局（ＡＡ）の事務代理機関として、属性証明書登録局（ＡＲＡ：Attribute Registration Authority）を設け、属性証明書登録局（ＡＲＡ）において、属性証明書（ＡＣ）の発行申請受理、申請者の審査、管理を行なう構成により、処理負荷の分散が可能である。

本発明の構成において適用されるグループ属性証明書（グループＡＣ）は、複数の対象、例えば複数のユーザ、あるいは複数のユーザ機器を１つの同一属性集合としたグループとして設定し、設定したグループを単位として、グループの構成機器または構成ユーザに対して発行される属性証明書である。グループ属性証明書は、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加された証明書である。

例えば複数人が所属している会社、組織、学校といった属性、あるいは家族といったグループに属する各ユーザまたはユーザ機器に対して発行される。あるいは、１つのサービスプロバイダの提供するサービスを受領する複数のユーザ単位といったグループのメンバ(ユーザ、ユーザ機器)に対して発行される。グループについては、様々な設定が可能であり、具体例については、後述する。

なお、後段で説明する実行属性証明書は、暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（Ａｄ）情報とを格納データとして有する。実行属性証明書の詳細については、後段で詳細に説明する。

属性証明書の基本フォーマットは ITU-T X.509 で規定されており，IETF PKIX WG で Profile を策定している。公開鍵証明書とは異なり所有者の公開鍵を含まない。しかし属性認証局(Attribute Certificate Authority)の署名がついているため、改竄されていないかどうかの判定はこの署名を検証することで行える、という点は公開鍵証明書と同様である。

なお、本発明において適用するグループ属性証明書、あるいは実行属性証明

書は、属性証明書の基本フォーマットに準拠したものとして構成可能である。ただし、ITU-T X.509 で規定されたフォーマットに従うことが必須ではなく、独自フォーマットとした属性証明書構成としてもよい。

本発明の構成においては、属性証明書（ＡＣ）の発行管理を行なう属性認証局(ＡＡ：Attribute Certificate Authority)、および属性証明書登録局（ＡＲＡ）の機能を、サービスプロバイダ、あるいはユーザデバイスが兼務することが可能である。すなわち、サービスプロバイダあるいはユーザデバイス自身が、属性認証局(ＡＡ)、属性証明書登録局（ＡＲＡ）の各機能を果たす構成が可能である。

属性証明書は基本的に公開鍵証明書と関連づけて利用する。すなわち属性証明書所有者の本人性自体は公開鍵証明書で確認し、その上で所有者にいかなる権限が与えられているかを属性証明書によって確認する。例えばサービスプロバイダがユーザ、あるいはユーザ機器に対するサービスを提供する際、サービスを受領する権利を有するか否かを属性証明書を検証して確認する。属性証明書の検証にあたっては、当該証明書の署名検証を行った後、その属性証明書に関連づけられている公開鍵証明書の検証も行う。

なお、その際、原則的には証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施することが好ましい。複数の認証局（ＣＡ）が存在し、階層構成をなす認証局構成では、下位の認証局自身の公開鍵証明書は、その公開鍵証明書を発行する上位認証局によって署名されている。すなわち、下層の認証局（ＣＡ－Ｌｏｗ）に対して上位の認証局（ＣＡ－Ｈｉｇｈ）が公開鍵証明書を発行するという連鎖的な公開鍵証明書発行構成をとる。公開鍵証明書の連鎖検証とは、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位（ルートＣＡ）までの公開鍵証明書の署名検証を行なうことを意味する。

属性証明書の有効期間を短期間とすることにより、失効処理を行わないことも可能である。この場合、証明書の失効手続きや失効情報の参照手順等を省くことができ、システムが簡易となる長所がある。ただし証明書の不正利用に対しては失効以外の何らかの対策が必要となるため、十分に注意しなければなら

ない。

図５を参照してグループ属性証明書の構成について説明する。

証明書のバージョン番号は、証明書フォーマットのバージョンを示す。

ＡＣ保持者の公開鍵証明書情報、これは属性証明書（ＡＣ）の発行者に対応する公開鍵証明書（ＰＫＣ）に関する情報であり、ＰＫＣ発行者名、ＰＫＣシリアル番号、ＰＫＣ発行者固有識別子等の情報であり、対応公開鍵証明書を関連づけるリンクデータとしての機能を持つ。

属性証明書の発行者の名前は、属性証明書の発行者、すなわち属性認証局（ＡＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

署名アルゴリズム識別子は、属性証明書の署名アルゴリズム識別子を記録するフィールドである。

証明書の有効期限は、証明書の有効期限である開始日時、終了日時が記録される。

属性情報フィールドには、グループ属性証明書のグループを識別するグループ識別情報としてグループＩＤが格納される。グループＩＤは、このグループ属性証明書を利用した権限確認を行なうサービスプロバイダの有するサービスプロバイダ（ＳＰ）管理グループ情報データベース（図５右下欄参照）のエントリと対応する識別子（ＩＤ）である。

サービスプロバイダの有するサービスプロバイダ（ＳＰ）管理グループ情報データベースは、図５右下欄に示すように、例えば、グループ属性証明書の発行者（ＡＲＡ）と、グループ識別子としてのグループ識別情報（グループＩＤ）、および「Ａ者の社員」、「Ｂさんの家族」といったグループ情報を対応付けたテーブルである。サービスプロバイダは、グループ証明書に基づく権限確認処理において、証明書格納データとしてのグループ識別情報（グループＩＤ）に基づいてテーブルから対応エントリを抽出し、グループ情報を含むグループ属性証明書情報を取得する。

なお、属性情報フィールドには、グループ識別情報（グループＩＤ）以外にも、様々な情報が格納可能であり、例えば、コンテンツ利用期限等のコンテン

ツ利用制限情報、サービス利用制限情報等の権限に関する詳細情報、さらにはサービスプロバイダ識別子（ＩＤ）、サービスプロバイダ・ネーム等の各種情報を格納することが可能である。また、詳細は、後述するが、暗号化コンテンツの復号に適用するコンテンツ鍵を取得するために必要となる情報を格納するフィールドとしての適用も可能である。

サービスプロバイダは、グループ属性証明書をユーザデバイスに対して送付し、ユーザデバイスは属性証明書の検証の後、自己のセキュリティチップ内のメモリに格納する。

属性証明書には、さらに、署名アルゴリズムが記録され、属性証明書発行者、例えば属性認証局（ＡＡ）によって署名が施される。発行者がサービスプロバイダ、あるいはユーザデバイスである場合は、各発行者の署名がなされる。電子署名は、属性証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行者の秘密鍵を用いて生成したデータである。

図６にグループ属性証明書（グループＡＣ）の発行者、所有者、検証者、属性情報の構成例を示す。例えば同一の会社、あるいは１つの家族に属するユーザの所有する複数のユーザ機器グループの各々に対してグループ属性証明書が発行される場合、発行されたグループ属性証明書は、ユーザの所有する機器内のセキュリティチップ（ＳＣ：Security Chip、あるいはＵＳＣ：User Security Chip）に格納される。ユーザデバイスの詳細については後述する。

ユーザデバイスに対して発行されたグループ属性証明書に基づいて権限確認を実行する検証者は、サービス提供エンティテイ、例えばサービスプロバイダの機器内のセキュリティモジュール（ＳＭ：Security Module）、あるいはユーザデバイスのセキュリティチップ（ＳＣ：Security Chip）である。なお、ユーザデバイスのセキュリティチップ、サービスプロバイダの機器内のセキュリティモジュールは、外部からのデータ読み出しの制限された耐タンパ構成を持つことが好ましい。

グループ属性証明書には、例えば同一の会社、あるいは１つの家族等を識別可能な識別情報としてのグループ識別情報（グループＩＤ）を属性情報として

有することとなる。

図７にグループ属性証明書の発行ポリシーテーブルの構成例を示す。グループ属性証明書の発行ポリシーテーブルは、グループ属性証明書を発行するエンティティ、例えば属性認証局(ＡＡ：Attribute Certificate Authority)、属性認証局(ＡＡ)の事務代行を行なう属性証明書登録局（ＡＲＡ：Attribute Registration Authority)、あるいはサービスプロバイダ、ユーザデバイスにおいて管理されるテーブルであり、発行したグループ属性証明書のグループ識別情報（グループＩＤ)、グループ情報、発行基準等の発行ポリシーとを対応付けたテーブルである。例えば、グループ属性証明書の新規発行、追加発行、更新処理等に際し、グループ属性証明書の発行ポリシーテーブルに基づいて、審査が実行され、ポリシーを満足する場合に限り、発行、更新等の手続きがなされる。

図８に権限管理システムに参加する各エンティティの信頼関係構成を説明するトラストモデルを示す。

システムホルダ（ＳＨ：System Holder）１３０は、本発明の権限管理システム全体の統括的管理を行なう主体、すなわちシステム運用主体であり、システムに参加する各エンティティのセキュリティチップ（ＳＣ)、セキュリティモジュール（ＳＭ）の正当性を保証するとともに、公開鍵証明書（ＰＫＣ）の発行責任を持つ。システムホルダ（ＳＨ）１３０は、最上位認証局としてのルートＣＡ（ＲｏｏｔＣＡ）１３１、階層構成の複数の認証局（ＣＡ）１３２、および公開鍵証明書発行事務局としての登録局（ＲＡ）１３３を有する。

システムホルダ（ＳＨ：System Holder）１３０は、属性認証局(ＡＡ)１４０、属性証明書登録局（ＡＲＡ）１５０、サービスプロバイダ１６０、およびユーザデバイス１７０としてのユーザ識別デバイス（ＵＩＤ：User Identification Device）１７１、エンドエンティテイ（ＥＥ：End Entity）１７２の各エンティテイに対応する公開鍵証明書（ＰＫＣ）を発行し、各エンティテイは、必要とするエンティテイの公開鍵証明書をそれぞれの機器内の耐タンパ構成を持つセキュリティチップ（ＳＣ）またはセキュリティモジュール（ＳＭ)、もしくは、場合によっては外部の記憶装置に公開鍵証明書（ＰＫＣ）

を格納する。

また、グループ属性証明書（グループＡＣ）は、サービスプロバイダ１６０、およびユーザデバイス１７０としてのユーザ識別デバイス（ＵＩＤ：User Identification Device）１７１、エンドエンティテイ（ＥＥ：End Entity）１７２の各エンティテイ等からの属性証明書発行要求を、例えば属性証明書登録局（ＡＲＡ）１５０において受領し、先に図７を参照して説明したポリシーテーブル１５１のポリシー（発行条件等）に従って属性証明書発行審査を行ない、発行可と判定された場合に属性認証局（ＡＡ）１４０に対して、属性証明書登録局（ＡＲＡ）１５０から発行依頼を転送する。

属性認証局（ＡＡ）１４０は、グループ属性証明書発行依頼に基づいて、グループ識別情報（グループＩＤ）を属性情報として格納し、属性認証局（ＡＡ）１４０の秘密鍵による署名を付加したグループ属性証明書（図５参照）を発行要求者に対して発行する。

なお、前述したように、これら属性認証局（ＡＡ）１４０、および属性証明書登録局（ＡＲＡ）１５０は、サービスプロバイダ、あるいはユーザデバイスがその機能を実行する構成とすることも可能である。

［（２）ユーザデバイス構成］

次にサービスを利用する情報処理装置としてのユーザデバイスの構成について説明する。ユーザデバイスは、その機能に基づいて、２つのカテゴリに分類される。一方はサービスを実際に利用する機器としてのエンドエンティテイ（ＥＥ）であり、サービスプロバイダの提供するサービス情報を受領するインタフェースを持つ例えばＰＣ、ホームサーバ、ＰＤＡ等の携帯端末、ＩＣカード等、各種データ処理装置である。これらの機器は、耐タンパ構成を持つセキュリティチップ（ＳＣ）またはモジュール（ＳＭ）を有し、機器対応の公開鍵証明書、機器対応のグループ属性証明書が必要に応じて格納される。

もう一方は、個人認証処理に適用するデバイスとしてのユーザ識別デバイス（ＵＩＤ）である。ユーザ識別デバイス（ＵＩＤ）もエンドエンティテイと同様の機器によって構成されるが、サービスプロバイダの提供するサービス情報

を直接受領するためのインタフェースを必ずしも有することのない機器である。サービスプロバイダ機器との通信は、エンドエンティテイ（ＥＥ）を介して実行する。ユーザ識別デバイス（ＵＩＤ）は、ユーザの認証に適用される機器である。これらの機器は、耐タンパ構成を持つセキュリティチップ（ＳＣ）またはセキュリティモジュール（ＳＭ）を有し、ユーザ対応の公開鍵証明書、機器対応のグループ属性証明書が必要に応じて格納される。

なお、エンドエンティテイ（ＥＥ）とユーザ識別デバイス（ＵＩＤ）は個別の機器としてそれぞれ構成することも可能であるが、１つの機器内に両機能を備えた構成とすることも可能である。

個別の構成具体例としては、例えばＩＣカード等の機器をユーザ識別デバイス（ＵＩＤ）として構成し、エンドエンティテイ（ＥＥ）をＰＣとした構成がある。この構成では、ＩＣカードをＰＣにデータ転送可能な状態にセットし、まずＩＣカードとサービスプロバイダ間との通信をＰＣを介して実行して公開鍵証明書、グループ属性証明書を適用したユーザ認証、ユーザ権限確認処理を実行し、さらにこれらの処理の後にエンドエンティテイとしてのＰＣとサービスプロバイダ間での認証、権限確認を行なう等の処理が実行可能となる。これらの権限確認処理の詳細については、後述する。

ユーザデバイスとしてのエンドエンティテイ（ＥＥ）とユーザ識別デバイス（ＵＩＤ）に構成されるセキュリテイチップの構成例について、図９を参照して説明する。なお、エンドエンティテイ（ＥＥ）は、データ処理手段としてのＣＰＵ、通信機能を備えた例えばＰＣ、ゲーム端末、携帯端末、ＰＤＡ、ＩＣカード（メモリカード）、ＤＶＤ，ＣＤ等の再生装置、記録再生装置等によって構成され、耐タンパ構造を持つセキュリティチップ（ＳＣ）が実装される。

図９に示すように、エンドエンティテイ（ＥＥ）またはユーザ識別デバイス（ＵＩＤ）により構成されるユーザデバイス２００には、セキュリティチップ２１０が、ユーザデバイス側制御部２２１に対して、相互にデータ転送可能な構成として内蔵される。

セキュリティチップ２１０は、プログラム実行機能、演算処理機能を持つＣＰＵ（Central Processing Unit）２０１を有し、データ通信用のインタフェ

ース機能を持つ通信インタフェース２０２、ＣＰＵ２０１によって実行される各種プログラム、例えば暗号処理プログラムなどを記憶するＲＯＭ(Read Only Memory) ２０３、実行プログラムのロード領域、また、各プログラム処理におけるワーク領域として機能するＲＡＭ (Random Access Memory) ２０４、外部機器との認証処理、電子署名の生成、検証処理、格納データの暗号化、復号化処理等の暗号処理を実行する暗号処理部２０５、サービスプロバイダ毎の情報、各種鍵データを含むデバイスの固有情報を格納した例えばＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)によって構成されるメモリ部２０６を有する。

ユーザデバイス２００は、暗号化コンテンツあるいはサービス情報等を格納する領域としてのＥＥＰＲＯＭ、ハードディスク等によって構成される外部メモリ部２２２を有する。外部メモリ部２２２は、公開鍵証明書、グループ属性証明書の格納領域としても利用可能である。

セキュリティチップを搭載したユーザデバイスが、外部エンティテイ、例えばサービスプロバイダと接続し、データ転送処理を実行する場合には、ネットワークインタフェース２３２を介したサービスプロバイダとの接続を実行する。ただし、前述したようにサービスプロバイダとの接続を実行するインタフェースを有するのは、エンドエンティテイ（ＥＥ）であり、ユーザ識別デバイス（ＵＩＤ）は、必ずしもネットワークインタフェース２３２を持つとは限らないので、ユーザ識別デバイス（ＵＩＤ）の接続機器インタフェース２３１を介してエンドエンティテイ(ＥＥ)の接続機器インタフェース２３１に接続し、エンドエンティテイのネットワークインタフェース２３２を介した通信を実行する。

すなわち、ユーザ識別デバイス（ＵＩＤ）は、エンドエンティテイを介してサービスプロバイダの機器との通信を実行する。

エンドエンティテイ（ＥＥ)、ユーザ識別デバイス（ＵＩＤ）等のユーザデバイスのセキュリティチップ２１０とサービスプロバイダ間でデータ転送を実行する場合には、必要に応じて、セキュリティチップ２１０と、外部エンティテイ間の相互認証が行われ、また転送データの暗号化が行なわれる。これら

の処理の詳細については、後段で詳述する。

ユーザデバイスのセキュリティチップの格納データ例を図１０に示す。これらの多くは、不揮発性メモリの一形態であるフラッシュメモリ等のＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)によって構成されるメモリ部２０６に格納されるが、公開鍵証明書、グループ属性証明書、あるいは後述する実行属性証明書は、セキュリティチップ内のメモリに格納しても、外部メモリに格納してもよい。

各データについて説明する。

公開鍵証明書（ＰＫＣ）：公開鍵証明書は、第三者に対して正当な公開鍵であることを示す証明書で、証明書には配布したい公開鍵を含み、信頼のおける認証局により電子署名がなされている。ユーザデバイスには、前述した階層構成の最上位認証局（ルートＣＡ）の公開鍵証明書、ユーザデバイスに対するサービスを提供するサービスプロバイダの公開鍵証明書等、ユーザデバイスとのデータ通信を実行する際の認証、暗号化、復号処理等に適用する公開鍵を取得するために必要となる公開鍵証明書が格納される。

グループ属性証明書（ＡＣ）：公開鍵証明書が証明書利用者（所有者）の“本人性”を示すのに対し、グループ属性証明書は証明書利用者のグループを識別しグループの構成メンバに付与された利用権限を確認するものである。利用者はグループ属性証明書を提示することにより、グループ属性証明書に記載された権利・権限情報に基づいて、サービス利用が行えるようになる。なお、グループ属性証明書は所定の発行手続きに基づいて発行されグループ属性証明書を受領した各エンティテイは、機器内の耐タンパ構成を持つセキュリティチップ（ＳＣ）またはセキュリティモジュール（ＳＭ)、もしくは、場合によっては外部の記憶装置に格納する。発行、格納処理の詳細は後述する。

実行属性証明書：暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（Ａｄ）情報とを格納データとして有する属性証明書であり、アドレス情報に基づいてユーザデバイス内メモリから取得する登録鍵を適用して暗号化実行命令を復号して実行命令を取得し、実行命令を

実行することで各種サービスが実行される。これらの処理の詳細は後述する。

鍵データ：鍵データとしては、セキュリティチップに対して設定される公開鍵、秘密鍵のペア、上述した実行属性証明書に格納された暗号化実行命令を復号する際に適用する登録鍵、登録鍵の破棄（リセット）処理に適用するリセット鍵、さらに、乱数生成用鍵、相互認証用鍵等が格納される。なお、登録鍵の格納領域は、あらかじめ決められたアドレスによって決定されるメモリ領域に格納される。登録鍵、リセット鍵については、後段で詳細に説明する。

識別情報：識別情報としては、セキュリティチップ自身の識別子としてのセキュリティチップＩＤが格納される。さらに継続的なサービス提供を受けるサービスプロバイダ（ＳＰ）の識別子としてのサービスプロバイダＩＤ、ユーザデバイスを利用するユーザに付与されたユーザＩＤ、サービスプロバイダの提供するサービスに対応するアプリケーションを識別するアプリケーションＩＤ等が格納可能である。

その他：ユーザデバイスには、さらに、乱数生成用のシード情報、すなわち認証処理、暗号処理等の際に適用する乱数をＡＮＳＩ　Ｘ９．１７に従って生成するための情報や、様々な利用制限が付加されたサービスに関する利用情報、例えば、コンテンツ利用回数制限が付加されたコンテンツを利用した際に更新されるコンテンツ利用回数情報、あるいは決済情報等の情報、あるいは、各情報に基づいて算出されるハッシュ値が格納される。

なお、図１０に示すデータ構成例は、一例であり、この他にも必要に応じて、ユーザデバイスの受領するサービスに関連する各種の情報が格納可能である。

なお、例えばサービス提供側のサービスプロバイダ側の有するセキュリティチップ、あるいはセキュリティモジュールも図９に示すユーザデバイスにおけるセキュリティチップ構成と同様の構成によって実現可能であり、以下に説明するグループ属性証明書の検証処理、生成処理、あるいは実行属性証明書の検証処理、生成処理の各実行手段として機能する。例えば、データ送受信部であるネットワークインタフェースを介して受信したグループ属性証明書あるいは実行属性証明書の検証処理の実行、あるいは、グループ属性証明書あるいは実行属性証明書の生成処理の実行手段として、図９に示すセキュリティチップ

とと同様の構成が適用可能である。

[（３）グループ属性証明書発行、利用処理]

次に、同一の学校、会社等の組織、あるいは１つの家族等、様々な集合に属するユーザ、あるいは、同一メーカの機器、同一サービスプロバイダのサービスを受領するユーザ、機器等、複数のユーザまたは機器をグループとして設定し、グループに属するユーザまたは機器の各々に対して発行するグループ属性証明書の発行処理、および利用処理について説明する。

グループ属性証明書は、サービスを受けようとするユーザまたは機器（ユーザデバイス）が特定のグループに属することを確認可能な証明書であり、サービス受領時等に、サービス提供エンティテイ、例えばサービスプロバイダに提示する。サービスプロバイダは、提示されたグループ属性証明書の検証処理を実行して、ユーザまたはユーザデバイスが特定のグループに属することが確認されたことを条件としてサービスを提供する。

グループ属性証明書は、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名を有する証明書である。

図１１にグループ属性証明書の発行申請、発行処理、利用処理の流れの概略を説明する図を示す。グループ属性証明書に基づいたグループ所属証明の確認を条件としたサービス提供を行なうサービスプロバイダ３１４の提供するサービスを受領しようとするユーザデバイス３１１、すなわちセキュリティチップを有するエンドエンティテイ（ＥＥ）またはユーザ識別デバイス（ＵＩＤ）は、まず、グループ属性証明書の発行エンティテイに発行要求を行なう。例えば、属性証明書登録局（ＡＲＡ：Attribute Registration Authority）３１２にグループ属性証明書の発行申請を行なう。

属性証明書登録局（ＡＲＡ）３１２は、発行申請に基づいて、発行ポリシーテーブル３１３を参照し、ポリシーを満足する場合には、属性認証局(ＡＡ：Attribute Certificate Authority)に対して属性証明書の発行を依頼し、属性認証局(ＡＡ)の発行したグループ属性証明書３１６をユーザデバイス３１１

に送信する。

グループ属性証明書３１６には、グループ識別子としてのグループＩＤが、属性情報フィールドに格納される（図５参照）。ユーザデバイス３１１は、サービスプロバイダ３１４の提供するサービス、例えばコンテンツ配信、決済処理等の何らかのサービスを受領する際に、グループ属性証明書３１６をサービスプロバイダ３１４に提示する。サービスプロバイダ３１４は、グループ属性証明書の検証処理、グループ情報データベース３１５の参照により、サービス提供を要求してきたユーザデバイス３１１がサービスを受領する権限を有するか否かを判定して、権限ありと判断した場合には、ユーザデバイス３１１に対するサービス提供を実行する。

以下、グループ属性証明書発行、利用処理について、

（３－１）グループ属性証明書発行前準備処理

（３－２）グループ属性証明書発行処理

（３－３）グループ属性証明書利用処理

以上、３項目について、順次説明する。

（３－１）グループ属性証明書発行前準備処理

まず、グループ属性証明書発行前準備処理について説明する。先に説明したように、グループ属性証明書は、基本的に属性認証局（ＡＡ）が発行し、属性証明書登録局（ＡＲＡ）が属性証明書発行要求エンティティからの発行要求を受理し、ポリシー審査等を実行して、発行可と判定した後、属性認証局（ＡＡ）に属性証明書発行要求を転送し、属性認証局（ＡＡ）の発行した属性証明書を属性証明書登録局（ＡＲＡ）を介して、発行要求エンティティに対して送付する処理構成が通常のスタイルである。ただし、以下、説明するように、サービスプロバイダ（ＳＰ）、ユーザデバイスにおいて、それぞれのポリシーの下に発行することも可能である。

本発明のグループ属性証明書は、識別可能なグループ、例えば家族、学校、会社、あるいは特定のメーカーの機器等、何らかのグループを特定した上で、そのグループ構成メンバ（機器またはユーザ）に対して発行するものであり、一方、サービスを提供するサービスプロバイダは、サービスを要求してきたユ

ーザまたは機器が、特定のグループに属するか否かをグループ属性証明書に基づいて判定する。従って、グループ属性証明書の発行処理実行エンティテイと、グループ属性証明書に基づく権限確認（検証処理）を実行しサービスを提供するエンティテイは、グループ属性証明書に対応して定義されるグループについて共通の認識を持つことが必要な場合、グループ属性証明書に対応して定義されるグループに関する情報、すなわちグループ情報を、グループ属性証明書発行エンティテイと、サービス提供エンティテイとが共有化する処理がグループ属性証明書発行前準備処理として必要となる。

以下、グループ属性証明書発行エンティテイを属性認証局（ＡＡ）または属性証明書登録局（ＡＲＡ）とし、サービス提供エンティテイをサービスプロバイダ（ＳＰ）とした場合のグループ情報共有化処理について、図１２を参照して説明する。

なお、以下に説明する例では、属性認証局（ＡＡ）と属性証明書登録局（ＡＲＡ）は信頼関係にあり、属性証明書登録局（ＡＲＡ）がグループ属性証明書の発行審査を行ない、属性証明書登録局（ＡＲＡ）の審査結果に基づいて、属性認証局（ＡＡ）がグループ属性証明書の発行処理を行なう構成を例として説明する。従って、グループ情報の共有エンティテイは、サービスプロバイダ（ＳＰ）と属性証明書登録局（ＡＲＡ）の２つのエンティテイとなる。

図１２に示す処理シーケンス図に従ってサービスプロバイダ（ＳＰ）と属性証明書登録局（ＡＲＡ）のグループ情報共有処理について説明する。

まずステップＳ１０１において、サービスプロバイダ（ＳＰ）とグループ属性証明書の発行審査を実行する属性証明書登録局（ＡＲＡ）との間で相互認証処理が実行される。なお、グループ属性証明書の発行審査を行なう属性証明書登録局（ＡＲＡ）を、以下、グループ属性証明書登録局（ＡＲＡ）とする。

サービスプロバイダ（ＳＰ）とグループ属性証明書登録局（ＡＲＡ）との間で実行される相互認証は、データ送受信を実行する２つのエンティテイ間で相互に相手が正しいデータ通信者であるか否かの確認のために実行される処理である。認証成立を条件として必要なデータ転送を行なう。また、相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として、

その後は、セッション鍵に基づく暗号化処理を施したデータ転送を行なう構成が好ましい。相互認証方式としては、公開鍵暗号方式、共通鍵暗号方式等、各方式の適用が可能である。

ここでは、公開鍵暗号方式の１つの認証処理方式であるハンドシェイクプロトコル（ＴＬＳ１．０）について図１３のシーケンス図を参照して説明する。

図１３において、エンティテイＡ（クライアント）、エンティテイＢ（サーバ）が、通信を実行する２エンティテイであり、ここではサービスプロバイダ（ＳＰ）またはグループ属性証明書登録局（ＡＲＡ）に対応する。まず、（１）エンティテイＢが暗号化仕様を決定するためのネゴシエーション開始要求をハローリクエストとしてエンティテイＡに送信する。（２）エンティテイＡはハローリクエストを受信すると、利用する暗号化アルゴリズム、セッションＩＤ、プロトコルバージョンの候補をクライアントハローとして、エンティテイＢ側に送信する。

（３）エンティテイＢ側は、利用を決定した暗号化アルゴリズム、セッションＩＤ、プロトコルバージョンをサーバーハローとしてエンティテイＡに送信する。（４）エンティテイＢは、自己の所有するルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式をエンティテイＡに送信（サーバ・サーティフィケート）する。なお、証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施しない場合には、必ずしもルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式を送付する必要はない。（５）エンティテイＢは、ＲＳＡ公開鍵またはＤｉｆｆｉｅ＆Ｈｅｌｌｍａｎ公開鍵情報をエンティテイＡに送信（サーバ・キー・エクスチェンジ）する。これは証明書が利用できない場合に一時的に適用する公開鍵情報である。

（６）次にエンティテイＢ側は、エンティテイＡに対してサーティフイケート・リクエストとして、エンティテイＡの有する証明書を要求し、（７）エンティテイＢによるネゴシエーション処理の終了を知らせる（サーバハロー終了）。

（８）サーバハロー終了を受信したエンティテイＡは、自己の所有するルートＣＡまでの公開鍵証明書（Ｘ．５０９ｖ３）一式をエンティテイＢに送信（ク

ライアント・サーティフィケート）する。なお、公開鍵証明書の連鎖検証を行なわない場合は公開鍵証明書の一式送付は必須ではない。（９）エンティテイＡは、４８バイト乱数をエンティテイＢの公開鍵で暗号化してエンティテイＢに送信する。エンティテイＢ、エンティテイＡは、この値をもとに送受信データ検証処理のためのメッセージ認証コード：ＭＡＣ（Message Authentication Code）生成用のデータ等を含むマスターシークレットを生成する。

（１０）エンティテイＡは、クライアント証明書の正しさを確認するため、ここまでのメッセージのダイジェストをクライアントの秘密鍵で暗号化してエンティテイＢに送信（クライアントサーティフィケート確認）し、（１１）先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（１２）認証の終了を通知する。一方、（１３）エンティテイＢ側からエンティテイＡに対しても、先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（１４）認証の終了を通知する。

上記処理において決定された暗号化アルゴリズムに従ってエンティテイＡとエンティテイＢ間のデータ転送が実行されることになる。

データ改竄の検証は、上述の認証処理でエンティテイＡとエンティテイＢ間の合意のもとに生成されたマスターシークレットから算出されるメッセージ認証コード：ＭＡＣ（Message Authentication Code）を各エンティテイの送信データに付加することでメッセージの改竄検証を行なう。

図１４にメッセージ認証コード：ＭＡＣ（Message Authentication Code）の生成構成を示す。データ送信側は、送信データに対して、認証処理において生成したマスターシークレットに基づいて生成されるＭＡＣシークレットを付加し、これらの全体データからハッシュ値を計算し、さらにＭＡＣシークレット、パディング、ハッシュ値に基づいてハッシュ算出を行なってメッセージ認証コード（ＭＡＣ）を生成する。この生成したＭＡＣを送信データに付加して、受信側で受信データに基づいて生成したＭＡＣと受信ＭＡＣとの一致が認められればデータ改竄なしと判定し、一致が認められない場合には、データの改竄があったものと判定する。

図１２に示すステップＳ１０１において、サービスプロバイダ（ＳＰ）とグループ属性証明書の発行審査を実行する属性証明書登録局（ＡＲＡ）との間で、例えば上述したシーケンスに従った相互認証処理が実行され、双方が正しい通信相手であることの確認がなされると、ステップＳ１０２において、サービスプロバイダ（ＳＰ）と、属性証明書登録局（ＡＲＡ）との間で、グループ情報の共有処理を実行する。

グループ情報の共有とは、具体的には、グループ属性証明書の発行エンティテイ（例えば属性証明書登録局（ＡＲＡ））の管理する発行ポリシーテーブルと、グループ属性証明書の検証および検証に基づくサービス提供エンティテイ（例えばサービスプロバイダ（ＳＰ））の有するグループ情報データベースとが整合した情報を保有する状態に設定する処理として行われる。

先に説明したように、グループ属性証明書の発行エンティテイ（例えば属性証明書登録局（ＡＲＡ））は、発行ポリシーテーブルを有し、グループ属性証明書の検証および検証に基づくサービス提供エンティテイ（例えばサービスプロバイダ（ＳＰ））は、グループ情報データベースを有する。図１５に各情報構成例を示す。

（Ａ）発行ポリシーテーブルは、属性証明書登録局（ＡＲＡ）が保持管理し、グループ属性証明書の発行処理等において参照する。一方、（Ｂ）グループ情報データベース（ＤＢ）は、サービスプロバイダ（ＳＰ）が保持管理し、サービス提供時のグループ属性証明書検証時に参照する。

属性証明書登録局（ＡＲＡ）が保持管理する（Ａ）発行ポリシーテーブルと、サービスプロバイダ（ＳＰ）が保持管理する（Ｂ）グループ情報データベース（ＤＢ）は、整合性を有することが必要となる。図１５の例では、（Ａ）発行ポリシーテーブルのエントリ３４１は、（Ｂ）グループ情報データベース（ＤＢ）のエントリ３５１と整合しており、（Ａ）発行ポリシーテーブルのエントリ３４２は、（Ｂ）グループ情報データベース（ＤＢ）のエントリ３５２と整合している。このように、属性証明書登録局（ＡＲＡ）が保持管理する（Ａ）発行ポリシーテーブルと、サービスプロバイダ（ＳＰ）が保持管理する（Ｂ）グループ情報データベース（ＤＢ）との整合性保持処理が図１２のシーケンス

図におけるステップＳ１０２のグループ情報共有処理である。

なお、グループ情報共有処理の態様としては、以下の２例がある。

ポリシー受諾型：グループ属性証明書の検証および検証に基づくサービス提供エンティテイ（例えばサービスプロバイダ（ＳＰ））は、種々のグループ属性証明書の発行エンティテイ（例えば属性証明書登録局（ＡＲＡ））の発行ポリシーを検討し、自身のサービスに適合するグループＡＲＡを選択し、その選択したグループＡＲＡが管理するグループ情報をサービスプロバイダ（ＳＰ）が取得する。

発行委託型：独自の属性証明書発行ポリシーを持たずに、単にグループ属性証明書の発行を請け負う形態のグループ属性証明書の発行エンティテイ（例えばグループ属性証明書登録局（ＡＲＡ））に対して、グループ属性証明書の検証および検証に基づくサービス提供エンティテイ（例えばサービスプロバイダ（ＳＰ））が設定した発行ポリシーをグループ属性証明書登録局（ＡＲＡ）に提示して、グループ属性証明書登録局（ＡＲＡ）が提示されたポリシーに従って、グループ属性証明書の発行処理を行なう。

具体的なグループ情報共有処理の形態としては、グループ属性証明書に関するグループＩＤ、発行者、グループ情報、発行ポリシー等の情報をグループ属性証明書の発行エンティテイ（例えばグループ属性証明書登録局（ＡＲＡ））が設定し、グループ属性証明書の検証および検証に基づくサービス提供エンティテイ（例えばサービスプロバイダ（ＳＰ））に提示して、双方のエンティテイが合意する態様、または、これらの情報をサービスプロバイダが設定し、グループＡＲＡに提示して、双方のエンティテイが合意する態様、あるいは、それぞれの情報を双方で分担して設定し、総合した情報に関して合意に至る態様、あるいはサービスプロバイダがグループ属性証明書登録局（ＡＲＡ）を一方的に信頼した態様等が可能である。

なお、発行委託型の場合には、新規なサービスプロバイダ（ＳＰ）が、グループ属性証明書を利用した新たなサービスを開始する場合には、属性証明書登録局（ＡＲＡ）がサービスプロバイダ（ＳＰ）自体の登録審査を行ない、その後に、上述のグループ情報共有処理を実行することになる。

ステップＳ１０２のグループ情報共有処理が終了すると、サービスプロバイダ（ＳＰ）は、ステップＳ１０３において、自己の管理するグループ情報データベースについて、合意した情報に基づくデータ更新処理を実行する。図１５に示すように、グループ情報データベースには、発行者、グループ識別情報（グループＩＤ）、グループ情報の各データが格納され、これらの情報に関するデータ登録、更新を実行する。一方、属性証明書登録局（ＡＲＡ）は、ステップＳ１０４において、自己の管理する発行ポリシーテーブルについて、合意した情報に基づくデータ更新処理を実行する。図１５に示すように、発行ポリシーテーブルには、グループＩＤ、グループ情報、発行ポリシーの各データが格納され、これらの情報に関するデータ登録、更新を実行する。

なお、上述した処理は、サービスプロバイダ（ＳＰ）と、属性証明書登録局（ＡＲＡ）とが、独立したエンティテイとして構成されている場合に必要となる処理であり、サービスプロバイダ（ＳＰ）が、属性証明書登録局（ＡＲＡ）を兼ねている場合は、サービスプロバイダ（ＳＰ）自身が、グループ情報データベースおよび発行ポリシーテーブルの両者を保持管理することになり、上述したサービスプロバイダ（ＳＰ）と、属性証明書登録局（ＡＲＡ）間でのグループ情報共有処理は省略可能となる。

また、上述した例は、グループ属性証明書の発行エンティテイをグループ属性証明書登録局（ＡＲＡ）とし、グループ属性証明書の検証および検証に基づくサービス提供エンティテイをサービスプロバイダ（ＳＰ）とした例を説明したが、それぞれのエンティテイの組み合わせに応じて、上述の処理が実行されることになる。

（３－２）グループ属性証明書発行処理

次に、グループ属性証明書発行処理について説明する。グループ属性証明書発行処理は、基本的には、属性認証局（ＡＡ）が実行することが原則である。ただし、サービスプロバイダ、ユーザデバイスにおいても独自の発行ポリシーに基づいて発行することが可能である。以下では、属性認証局（ＡＡ）によるグループ属性証明書の発行処理シーケンスについて説明する。

属性証明書登録局（ＡＲＡ）が属性証明書発行要求エンティテイからの発行

要求を受理し、ポリシー審査等を実行して、発行可と判定した後、属性認証局（ＡＡ）に属性証明書発行要求を転送し、属性認証局（ＡＡ）の発行した属性証明書を属性証明書登録局（ＡＲＡ）を介して、発行要求エンティテイに対して送付する処理構成が通常の属性証明書発行シーケンスである。

図１６を参照して、ユーザデバイスであるエンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）がグループ属性証明書の発行要求主体である場合の処理について説明する。なお、図１６において、

ＵＩＤ：ユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：ＵＩＤ内に構成されるユーザセキュリティチップ、

ＥＥ：エンドエンティテイ（ユーザデバイス）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

グループＡＲＡ：グループ属性証明書登録局制御部、

グループＡＡ：グループ属性認証局制御部、

である。

まず、ステップＳ１１１において、ユーザがエンドエンティテイ（ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）の発行要求コマンドを入力する。この際、ユーザはグループ属性証明書発行に必要となる属性値を入力する。属性値は、グループＩＤ、あるいはグループに属することを証明する情報等である。

エンドエンティテイ（ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）の発行要求の入力を受領すると、ステップＳ１１２において、エンドエンティテイ（ＥＥ）は、グループＡＲＡに対する接続要求を行ない、一方、ステップＳ１１３において、エンドエンティテイ（ＥＥ）内のセキュリティチップ（ＳＣ）に対して、相互認証開始要求を出力する。

ステップＳ１１４において、セキュリティチップと、グループＡＲＡ間の相互認証が実行される。これは例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ１１５では、セキュリティチップからエンドエンティテイに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中

止される。相互認証が成立すると、ステップＳ１１６において、エンドエンティテイ（ＥＥ）は、グループＡＲＡに対してグループ属性証明書（Ｇｐ．ＡＣ）発行要求を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）発行要求には、エンドエンティテイ情報、属性値（例えばグループＩＤ、グループ情報）が含まれる。

エンドエンティテイ（ＥＥ）からグループ属性証明書（Ｇｐ．ＡＣ）発行要求を受信したグループＡＲＡは、ステップＳ１１７において、発行ポリシーテーブルを参照して、ポリシーに準拠したグループ属性証明書の発行が可能か否かを判定し、可であれば、ステップＳ１１８に進み、不可であれば、発行不可メッセージをエンドエンティテイに通知する。

ステップＳ１１８では、グループＡＲＡが属性値（グループＩＤ）を伴うグループ属性証明書（Ｇｐ．ＡＣ）発行要求をグループＡＡに送信し、ステップＳ１１９において、グループＡＡが、グループＩＤを属性情報として格納し、電子署名を施したグループ属性証明書（図５参照）を生成し、グループＡＲＡに送信する。

ステップＳ１２０において、グループＡＲＡが、発行されたグループ属性証明書（Ｇｐ．ＡＣ）をエンドエンティテイ（ＥＥ）に送信する。エンドエンティテイ（ＥＥ）は、受信したグループ属性証明書（Ｇｐ．ＡＣ）をメモリに格納する。この際、グループ属性証明書（Ｇｐ．ＡＣ）の電子署名の検証を実行して、改竄の無いことを確認した後。メモリに格納する。

グループ属性証明書の生成時にグループＡＡが実行する電子署名の生成、および、グループ属性証明書の格納時にエンドエンティテイが実行する電子署名の検証処理について、図１７、図１８を参照して説明する。

署名は、データ改竄の検証を可能とするために付加されるものであり、前述のＭＡＣ値を用いることも可能であり、公開鍵暗号方式を用いた電子署名を適用することも可能である。

まず、公開鍵暗号方式を用いた電子署名の生成方法について、図１７を用いて説明する。図１７に示す処理は、ＥＣ－ＤＳＡ（(Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3）を用いた電子署名データの生成処理

フローである。なお、ここでは公開鍵暗号として楕円曲線暗号(Elliptic Curve Cryptosystem（以下、ＥＣＣと呼ぶ)）を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号((Rivest、Shamir、Adleman)など(ANSI X9.31))を用いることも可能である。

図１７の各ステップについて説明する。ステップＳ１において、ｐを標数、a、ｂを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$，$4a^3+27b^2\neq 0$（ｍｏｄ　ｐ))、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージＭのハッシュ値を計算し、f=Hash(M)とする。

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

P=(Ｘａ，Ｙａ),Q=(Ｘｂ，Ｙｂ),R=(Ｘｃ,Ｙｃ)=P+Q とすると、

P≠Q の時（加算)、

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

P=Q の時（2倍算)、

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$

これらを用いて点Gのu倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。G、2×G、4×G・・を計算し、uを2進数展開して1が立っているところに対応する$2^i\times G$(Gをi回2倍算した値(iはuのＬＳＢから数えた時のビット位置)）を加算する。

ステップＳ５で、ｃ＝Ｘｖｍｏｄ ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［(ｆ＋ｃＫｓ）／ｕ］ｍｏｄ ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図１８を用いて説明する。ステップＳ１１で、Ｍをメッセージ、ｐを標数、ａ、ｂを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$，$4a^3+27b^2\neq 0$ (ｍｏｄ ｐ))、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Ｇを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージＭのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４で $h=1/d \bmod r$ を計算し、ステップＳ１５でｈ１＝ｆｈ ｍｏｄ ｒ、ｈ２＝ｃｈ ｍｏｄ ｒを計算する。

ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、ベースポイントＧおよびＫｓ×Ｇを知っているので、図１７のステップＳ４と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実

際には、無限遠点の判定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であることが判明している）。ステップＳ１８でＸｐ ｍｏｄ ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Ｐが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ ｍｏｄ ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。上述したように、署名付けやハッシュをとるだけでは改竄は可能であるが、検出により実質的に改竄できないことと同様の効果がある。

次に、図１９を参照して、ユーザ識別デバイス（ＵＩＤ）内のユーザセキュリティチップ（ＵＳＣ）対応のグループ属性証明書を発行する手順について説明する。先に説明したように、ＵＩＤは、エンドエンティテイ（ＥＥ）を介して外部と通信が可能な構成であるので、属性証明書の取得処理もエンドエンティテイ（ＥＥ）を介して実行される。

ステップＳ１３１～Ｓ１３５の処理は、図１６を参照して説明したステップＳ１１１～Ｓ１１５の処理と同様の処理であり、説明を省略する。

ステップＳ１３４におけるエンドエンティテイ内のセキュリティチップ（ＳＣ）とグループＡＲＡ間の相互認証が成立すると、ステップＳ１３７において、ユーザ識別デバイス（ＵＩＤ）内のユーザセキュリティチップ（ＵＳＣ）と、エンドエンティテイ内のセキュリティチップ（ＳＣ）との間における相互認証処理が実行される。この認証処理は、エンドエンティテイ（ＥＥ）と、ユーザ

識別デバイス（ＵＩＤ）との接続機器インタフェース２３１（図９参照）を介して実行される。この認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参照）を中心とした処理として先に図１３を参照して説明した公開鍵方式に基づく認証処理として実行可能である。ステップＳ１３８において、認証の成立情報を含む認証完了通知がエンドエンティテイ（ＥＥ）に通知され、認証成立を条件として次ステップに進む。

ステップＳ１３９では、エンドエンティテイ（ＥＥ）からユーザセキュリティチップ（ＵＳＣ）相互認証開始要求が出力され、ステップＳ１４０において、ＵＳＣと、グループＡＲＡ間の相互認証処理が実行される。ステップＳ１４１において、認証の成立情報を含む認証完了通知がＵＳＣからエンドエンティテイ（ＥＥ）に通知され、認証成立を条件として、エンドエンティテイ（ＥＥ）は、ステップＳ１４２において、グループＡＲＡに対してグループ属性証明書（Ｇｐ．ＡＣ）発行要求を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）発行要求には、エンドエンティテイ情報、属性値（例えばグループＩＤ、グループ情報）が含まれる。

エンドエンティテイ（ＥＥ）からグループ属性証明書（Ｇｐ．ＡＣ）発行要求を受信したグループＡＲＡは、ステップＳ１４３において、発行ポリシーテーブルを参照して、ポリシーに準拠したグループ属性証明書の発行が可能か否かを判定し、可であれば、ステップＳ１４４に進み、不可であれば、発行不可メッセージをエンドエンティテイに通知する。

ステップＳ１４４では、グループＡＲＡが属性値（グループＩＤ）を伴うグループ属性証明書（Ｇｐ．ＡＣ）発行要求をグループＡＡに送信し、ステップＳ１４５において、グループＡＡが、グループＩＤを属性情報として格納し、電子署名を施したグループ属性証明書（図５参照）を生成し、グループＡＲＡに送信する。

ステップＳ１４６において、グループＡＲＡが、発行されたグループ属性証明書（Ｇｐ．ＡＣ）をエンドエンティテイ（ＥＥ）を介してＵＩＤに送信する。ＵＩＤは、受信したグループ属性証明書（Ｇｐ．ＡＣ）をメモリに格納する。この際、グループ属性証明書（Ｇｐ．ＡＣ）の電子署名の検証を実行して、改

竄の無いことを確認した後、メモリに格納する。

上述したように、ダイレクトにグループＡＲＡとの通信機能を持たないユーザ識別デバイス（ＵＩＤ）がユーザセキュリティチップ（ＵＳＣ）に対応するグループ属性証明書を取得するためには、エンドエンティテイ（ＥＥ）を介する処理が必要となる。その際、ユーザセキュリティチップ（ＵＳＣ）とグループＡＲＡとの間で相互に認証を行なうためには、たとえば、

（１）ＥＥのＳＣとグループＡＲＡとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとグループＡＲＡとの相互認証、

のすべてが成立することが条件となる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

（３－３）グループ属性証明書利用処理

ユーザデバイス内のセキュリティチップ（ＳＣ）、あるいはユーザセキュリティチップ（ＵＳＣ）に格納したグループ属性証明書を利用した処理について説明する。なお、ここでは、具体的なサービス形態については言及せず、サービス提供開始に至るまでのグループ属性証明書に基づくサービス利用権限確認処理について説明する。具体的なサービス形態については、後段の別項目において説明する。

図２０以下を参照して、ユーザデバイスとしてのエンドエンティテイ（ＥＥ）内のセキュリティチップ（ＳＣ）に対して発行されたグループ属性証明書を利用したサービス利用権限確認を含むサービス開始までの処理について説明する。なお、図２０において、

ＵＩＤ：ユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：ＵＩＤ内に構成されるユーザセキュリティチップ、

ＥＥ：エンドエンティテイ（ユーザデバイス）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

ＳＰ：サービスプロバイダ制御部、

ＳＭ：ＳＰ内のセキュリティモジュール、

である。

なお、ユーザデバイス（ＥＥ）のセキュリティチップ（ＳＣ）、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）、およびサービスプロバイダ（ＳＰ）のセキュリティモジュールは、例えば先に説明した図９のセキュリティチップと同様の構成を持つ。

まず、ステップＳ１５１において、ユーザがエンドエンティテイ（ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）の利用要求コマンドを入力する。この際、ユーザは利用するグループ属性証明書に設定されたグループＩＤを指定する。ただし、特定のサービスを指定することにより唯一のグループＩＤが決定可能である場合は、サービスの指定のみとしてもよい。

エンドエンティテイ（ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）の利用要求入力を受領すると、ステップＳ１５２において、エンドエンティテイ（ＥＥ）は、サービスプロバイダ（ＳＰ）に対する接続要求を行ない、一方、ステップＳ１５３において、エンドエンティテイ（ＥＥ）内のセキュリティチップ（ＳＣ）に対して、相互認証開始要求を出力する。

ステップＳ１５４において、セキュリティチップと、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。これは、セキュリティチップと、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）内に構成される、例えば図９に示す暗号処理部２０５を中心とした処理として、例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。

ステップＳ１５５では、セキュリティチップからエンドエンティテイに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ１５６において、エンドエンティテイ（ＥＥ）は、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対して自己のメモリに格納

したグループ属性証明書（Ｇｐ．ＡＣ）を送信する。なお、グループ属性証明書（Ｇｐ．ＡＣ）の送信は、サービスプロバイダ（ＳＰ）からの送信要求に応答する形で実行する構成としてもよい。また、エンドエンティテイ（ＥＥ）は、グループ属性証明書（Ｇｐ．ＡＣ）の送信に併せて、グループ属性証明書（Ｇｐ．ＡＣ）の利用要求を行なう場合もある。このグループ属性証明書（Ｇｐ．ＡＣ）には、グループ識別情報（グループＩＤ）が属性値として格納されている。

サービスプロバイダは、例えば図９に示すユーザデバイスと同様の構成を持つネットワークインタフェースを受信部として、エンドエンティテイ（ＥＥ）からグループ属性証明書（Ｇｐ．ＡＣ）を受信し、セキュリティモジュール（ＳＭ）に転送する。セキュリティモジュール（ＳＭ）は、ステップＳ１５７において、グループ属性証明書検証処理を実行する。セキュリティモジュールは、先に説明したように、図９に示すユーザデバイスのセキュリティチップと同様の構成を持ち、セキュリティモジュールが、グループ属性証明書検証処理部として機能することになる。

グループ属性証明書の検証処理の詳細について、図２１乃至図２３を参照して説明する。まず、属性証明書（ＡＣ）と公開鍵証明書（ＰＫＣ）との関連確認処理について、図２１を参照して説明する。図２１のフローは、属性証明書（ＡＣ）の検証を実行する際に行なわれる属性証明書（ＡＣ）に関連する公開鍵証明書（ＰＫＣ）の確認処理である。

確認対象の属性証明書（ＡＣ）がセット（Ｓ２１）されると、属性証明書のＡＣ保持者の公開鍵証明書情報（ホルダー）フィールドを抽出（Ｓ２２）し、抽出した公開鍵証明書情報（ホルダー）フィールド内に格納された公開鍵証明書の発行者情報（ＰＫＣ発行者）、公開鍵証明書シリアル番号（ＰＫＣシリアル）を確認（Ｓ２３）し、公開鍵証明書の発行者情報（ＰＫＣ発行者）、公開鍵証明書シリアル番号（ＰＫＣシリアル）に基づいて公開鍵証明書（ＰＫＣ）を検索（Ｓ２４）して、属性証明書（ＡＣ）に関連付けられた公開鍵証明書（ＰＫＣ）を取得（Ｓ２５）する。

図２１に示すように、属性証明書（ＡＣ）と公開鍵証明書（ＰＫＣ）とは、

属性証明書に格納された公開鍵証明書情報（ホルダー）フィールド内の公開鍵証明書発行者情報（ＰＫＣ発行者）、および公開鍵証明書シリアル番号（ＰＫＣシリアル）により関連付けがなされている。

次に、図２２を参照して属性証明書（ＡＣ）の検証処理について説明する。まず、検証対象となる属性証明書（ＡＣ）をセット（Ｓ５１）し、属性証明書（ＡＣ）格納情報に基づいて、属性証明書（ＡＣ）の所有者および署名者を特定（Ｓ５２）する。さらに、属性証明書（ＡＣ）の所有者の公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ５３）して、公開鍵証明書の検証処理を実行（Ｓ５４）する。

図２３を参照して公開鍵証明書（ＰＫＣ）の検証処理について説明する。図２３に示す公開鍵証明書（ＰＫＣ）の検証は、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位（ルートＣＡ）までの公開鍵証明書の署名検証を行なう連鎖検証処理フローである。まず、検証対象となる公開鍵証明書（ＰＫＣ）をセット（Ｓ３１）し、公開鍵証明書（ＰＫＣ）格納情報に基づいて、公開鍵証明書（ＰＫＣ）署名者を特定（Ｓ３２）する。さらに、検証対象となる証明書連鎖の最上位の公開鍵証明書であるかを判定（Ｓ３３）し、最上位でない場合は、最上位公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ３４）する。最上位公開鍵証明書が取得されセット（Ｓ３５）されると、署名検証に必要な検証鍵（公開鍵）を取得（Ｓ３６）し、検証対象の署名が自己署名であるか否かを判定し（Ｓ３７）、自己署名でない場合は、下位ＰＫＣをセット（Ｓ３９）して、上位の公開鍵証明書から取得した検証鍵（公開鍵）に基づいて署名検証を実行（Ｓ４０）する。なお、ステップＳ３７における自己署名判定において、自己署名の場合は自己の公開鍵を検証鍵とした検証を実行（Ｓ３８）し、ステップＳ４１に進む。

署名検証に成功した場合（Ｓ４１：Ｙｅｓ）は、目的とするＰＫＣの検証が完了したか否かを判定（Ｓ４２）し、完了している場合は、ＰＫＣ検証を終了する。完了していない場合は、ステップＳ３６に戻り、署名検証に必要な検証鍵（公開鍵）の取得、下位の公開鍵証明書の署名検証を繰り返し実行する。なお、署名検証に失敗した場合（Ｓ４１：Ｎｏ）は、ステップＳ４３に進み、エ

ラー処理、例えばその後の手続きを停止する等の処理を実行する。

図２２に戻り、属性証明書検証処理の説明を続ける。図２３で説明した公開鍵証明書の検証に失敗した場合（Ｓ５５でＮｏ）は、ステップＳ５６に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ５５でＹｅｓ）は、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書を直接あるいはリポジトリなどから取得（Ｓ５７）して、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書の検証処理を実行（Ｓ５８）する。

属性証明書（ＡＣ）の署名者に対応する公開鍵証明書の検証に失敗した場合（Ｓ５９でＮｏ）は、ステップＳ６０に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合（Ｓ５９でＹｅｓ）は、属性証明書（ＡＣ）の署名者に対応する公開鍵証明書から公開鍵を取り出し（Ｓ６１）て、取り出した公開鍵を用いて属性証明書（ＡＣ）の署名検証処理を実行（Ｓ６２）する。署名検証に失敗した場合（Ｓ６３でＮｏ）は、ステップＳ６４に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合（Ｓ６３でＹｅｓ）は、属性証明書検証を終了し、その後の処理、すなわちサービス提供のために実行すべきその他の条件確認処理に移行する。

図２０のシーケンス図に戻って説明を続ける。ステップＳ１５７のグループ属性証明書（Ｇｐ．ＡＣ）の検証が上述した処理によって実行されると、セキュリティモジュール（ＳＭ）は、検証結果をサービスプロバイダ（ＳＰ）に出力し、検証不成功の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティティに通知する処理を実行してもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ１６１に進む。ステップＳ１６１以下の処理を図２４を参照して説明する。ステップＳ１６１では、グループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、サービスプロバイダの保有するグループ情報データベースに基づいて実行する。

グループ属性証明書（Ｇｐ．ＡＣ）の審査処理について、図２５を参照して説明する。ステップＳ１６１－１において、サービスプロバイダ（ＳＰ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）から発行者情報を取得する。さらに、ステップＳ１６１－２において、属性フィールドから属性値、すなわちグループ識別情報（グループＩＤ）を取得する。

ステップＳ１６１－３において、グループ属性証明書（Ｇｐ．ＡＣ）から取得したＡＣ発行者、およびグループＩＤに基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、ステップＳ１６１－４において、グループ情報データベースからグループ情報を取得する。

図２４のシーケンス図に戻り説明を続ける。グループ属性証明書（Ｇｐ．ＡＣ）に対応するグループ情報が登録されていない場合、あるいはユーザがグループ情報に示された条件を満足していない場合は、審査不成功（Ｓ１６２：Ｎｏ）となり、ステップＳ１６３のエラー処理を実行する。例えばグループＡＣの審査不成立であり、サービス実行ができない旨のメッセージをエンドエンティテイ（ＥＥ）に通知する。また、サービス提供に際して複数のグループ属性証明書の検証・審査が必要な場合は、この条件をサービス情報データベースで管理する。

なお、サービス情報データベースは、サービスを提供するにあたり、どのグループＡＣが必要であるかという情報を格納しているデータベースである。ただし、前述したグループ情報データベースとサービス情報データベースを各々個別に保有することは必須ではなく、グループ情報データベースとサービス情報データベースとを融合あるいはリンクさせたデータベース構成を持つことが可能である。すなわち、サービス提供にどのグループＡＣが必要であるかというデータを、前述のグループ情報データベース、あるいはグループ情報データベースのリンク情報から取得する構成も可能である。以下の説明において、グループ情報データベースは、サービス情報データベースとしての機能も併せ持つものとして説明する。

図２４のシーケンス図に戻り説明を続ける。審査成功（Ｓ１６２：Ｙｅｓ）

の場合は、サービス実行のための他の条件の必要性の有無を判定する。この条件は、サービスプロバイダが任意に設定可能な条件である。さらに、ステップＳ１６５において、サービス提供のために他のグループ属性証明書が必要であるか否かを判定する。

これは、図２６に示すように、サービスを提供条件として、ユーザあるいはユーザ機器が異なる複数のグループに属することが条件とされる場合を想定したものである。例えば、図２６（ａ）に示すように、２つの異なるグループに属することの証明により、サービスを提供するという設定ができる。

具体的には、例えばユーザの居住地が特定の地域に属することを証明するグループ属性証明書Ａ（グループＡ）と、ユーザ機器が特定メーカーの機器であることを示すグループ属性証明書Ｂ（グループＢ）との２つのグループ属性証明書の提示、検証によりサービスを提供するといった設定である。

さらに、図２６（ｂ）に示すように、３つ以上の異なるグループに属することの証明により、サービスを提供するという設定もできる。具体的には、例えばユーザの居住地が特定の地域に属することを証明するグループ属性証明書Ａ（グループＡ）と、ユーザ機器が特定メーカーの機器であることを示すグループ属性証明書Ｂ（グループＢ）と、さらに、ユーザの年齢が所定の範囲に属することを示すグループ属性証明書Ｃ（グループＣ）の３つのグループ属性証明書の提示、検証によりサービスを提供するといった設定である。

このように、ユーザあるいはユーザ機器に対して発行された異なる２以上のグループ属性証明書を適用して、ユーザあるいはユーザ機器が複数の異なるグループに属していることの検証を条件としたサービス提供を行なう場合、サービスプロバイダ（ＳＰ）は、ステップＳ１６６において、エンドエンティテイ（ＥＥ）に対して他のグループ属性証明書（Ｇｐ．ＡＣ）の提示を要求する。他のグループ属性証明書の提示を求められたエンドエンティテイ（ＥＥ）は、ステップＳ１６７において、求めに応じたグループ属性証明書をサービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に送信する。セキュリティモジュール（ＳＭ）はエンドエンティテイ（ＥＥ）から受信した新たなグループ属性証明書について、図２０に示すステップＳ１５７以下の処理、すなわち、

グループ属性証明書の検証処理、審査処理等を実行する。

サービス提供に必要となるグループ属性証明書の検証、審査に成功したことを条件として、ステップＳ１６８においてサービス提供が実行される。このサービスは、サービスプロバイダの提供するコンテンツ配信、決済処理、ユーザデバイスとしての機器（例えば家電機器）のリモートコントロール、リモートメンテナンス処理、コミュニュケーションサービス等、様々である。これらサービスの具体例については、後段で説明する。

次に、図２７、図２８を参照して、ユーザデバイスとしてのユーザ識別デバイス（ＵＩＤ）内のユーザセキュリティチップ（ＵＳＣ）に対応して発行されたグループ属性証明書に基づくサービス提供までの処理について説明する。ユーザ識別デバイス（ＵＩＤ）は個人識別デバイスとして機能する機器である。グループ属性証明書は、エンドエンティテイおよびユーザ識別デバイス各々に対して個別に発行可能である。基本的には、ユーザ識別デバイスに発行されるグループ属性証明書は、ユーザ自体がある特定のグループのメンバであるか否かの確認を可能とする証明書として発行される。ＵＩＤは、エンドエンティテイ（ＥＥ）を介して外部と通信が可能な構成であるので、属性証明書の利用処理もエンドエンティテイ（ＥＥ）を介して実行される。

図２７において、ステップＳ１７１～Ｓ１７５は、図２０に示すステップＳ１５１～Ｓ１５５と同様の処理、すなわち、エンドエンティテイ（ＥＥ）内のセキュリティチップ（ＳＣ）とサービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証を中心とした処理である。

ステップＳ１７４に示すエンドエンティテイ内のセキュリティチップ（ＳＣ）とサービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が成立すると、ステップＳ１７７において、ユーザ識別デバイス（ＵＩＤ）内のユーザセキュリティチップ（ＵＳＣ）と、エンドエンティテイ内のセキュリティチップ（ＳＣ）との間における相互認証処理が実行される。この認証処理は、エンドエンティテイ（ＥＥ）と、ユーザ識別デバイス（ＵＩＤ）との接続機器インタフェース２３１（図９参照）を介して実行される。この認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参

照)を中心とした処理として先に図１３を参照して説明した公開鍵方式に基づく認証処理として実行可能である。ステップＳ１７８において、認証の成立情報を含む認証完了通知がエンドエンティテイ（ＥＥ）に通知され、認証成立を条件として次ステップに進む。

ステップＳ１７９では、エンドエンティテイ（ＥＥ）からユーザセキュリティチップ（ＵＳＣ）に相互認証開始要求が出力され、ステップＳ１８０において、ＵＳＣと、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証処理が実行される。ステップＳ１８１において、認証の成立情報を含む認証完了通知がＵＳＣからエンドエンティテイ（ＥＥ）に通知され、認証成立を条件として、ユーザ識別デバイス（ＵＩＤ）は、ステップＳ１８２において、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対してグループ属性証明書（Ｇｐ．ＡＣ）を提示する。このグループ属性証明書（Ｇｐ．ＡＣ）は、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ(ＵＳＣ)に対応して発行されたグループ属性証明書(Ｇｐ．ＡＣ)である。

ユーザセキュリティチップ(ＵＳＣ)からグループ属性証明書(Ｇｐ．ＡＣ)を受信したサービスプロバイダ(ＳＰ)のセキュリティモジュール(ＳＭ)は、ステップＳ１８３において、受信したグループ属性証明書の検証処理を実行する。この検証処理は、図２１～図２３を参照して説明したと同様の処理である。以下、ステップＳ１８４～ステップＳ１９８（図２８）の処理は、図２０および図２４を用いて説明したエンドエンティテイのセキュリティチップ（ＳＣ）対応のグループ属性証明書に対する処理と基本的に同様であるので説明を省略する。ただし、図２８に示すステップＳ１９７では、新たなグループ属性証明書の送信は、ユーザ識別デバイス（ＵＩＤ）が実行することになる。

上述したように、ダイレクトにサービスプロバイダ（ＳＰ）との通信機能を持たないユーザ識別デバイス(ＵＩＤ)がユーザセキュリティチップ(ＵＳＣ)に対応するグループ属性証明書の利用を行なうためには、エンドエンティテイ（ＥＥ）を介する処理が必要となる。その際、ユーザセキュリティチップ（ＵＳＣ）とサービスプロバイダ（ＳＰ）との間で相互に認証を行なうためには、たとえば、

（１）ＥＥのＳＣとサービスプロバイダ（ＳＰ）との相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとサービスプロバイダ（ＳＰ）との相互認証、

のすべてが成立することが条件となる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

なお、図２０および図２４では、エンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）対応のグループ属性証明書を利用した処理を説明し、図２７、図２８では、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）に対応して発行されたグループ属性証明書を利用した処理を説明したが、エンドエンティテイ（ＥＥ）のセキュリテイチップ（ＳＣ）対応のグループ属性証明書と、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）に対応して発行されたグループ属性証明書との双方の複数の属性証明書の検証および審査に基づいてサービスを提供する構成、例えば先に図２６を参照して説明したような構成も可能である。この場合は、図２７、図２８に示す処理と、図２０、図２４に示す処理とを組み合わせた処理を実行することになる。

例えば、サービスプロバイダは、ユーザデバイスとしてのエンドエンティテイ（機器）をグループのメンバとしたグループ定義に基づく第１のグループ属性証明書から取得される第１のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行うとともに、ユーザ識別デバイスから送付されるユーザをグループのメンバとしたグループ定義に基づく第２のグループ属性証明書から取得される第２のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行する構成が可能である。

[（４）ユーザデバイス間におけるグループ属性証明書の発行、利用処理]

上述した説明において、グループ属性証明書は、主としてサービスプロバイダがユーザデバイスに対して提供するサービスの利用権限を確認するための証明書として適用するものとして説明した。グループ属性証明書の発行主体は、基本的には、グループ属性認証局（グループＡＡ）であるが、サービスプロバイダ（ＳＰ）がグループ属性認証局（グループＡＡ）およびグループＡＲＡの機能を実行し、サービスプロバイダ（ＳＰ）が独自のポリシーの下にグループ属性証明書を発行する形態も可能である。さらにユーザデバイス自身がグループ属性認証局（グループＡＡ）およびグループＡＲＡの機能を実行し、ユーザデバイスが独自のポリシーの下にグループ属性証明書を発行する形態も可能である。以下、ユーザデバイスがグループ属性証明書を発行し、ユーザデバイスに対するアクセス制限をグループ属性証明書を利用して実行する構成について説明する。

具体的な利用形態としては、例えば通信機能を有する通信処理装置としてのユーザデバイス（エンドエンティテイ）が特定のメンバーからのアクセスのみを許可したい場合、特定メンバーをグループとして設定したグループ属性証明書を発行して、アクセスを要求してきた他のユーザデバイスから、その発行済みのグループ属性証明書の提示を求めて、提示されたグループ属性証明書の検証を実行して、アクセスを許可するアクセス権限管理形態がある。

このサービス提供形態、すなわちアクセス許可サービスの提供形態は、サービスプロバイダ（ＳＰ）がグループ属性証明書を発行する構成も可能であるが、ユーザデバイスにおいて、例えば特定の友人、家族、同一の会社、学校等のメンバー等をグループとして設定し、設定したグループに対応するグループ識別情報として格納してグループ属性証明書を生成して発行することにより、個人ベースでのアクセス管理が可能となる。

まず、図２９を参照して、ユーザデバイス間においてグループ属性証明書を発行し、格納する処理について説明する。

図２９において、ユーザデバイスである通信処理装置としてのエンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）がグループ属性証明書の発行要

求主体である場合の処理について説明する。なお、図２９において、

ＵＩＤ：アクセス要求元ユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：アクセス要求元ＵＩＤ内に構成されるユーザセキュリティチップ、

アクセス元ＥＥ：アクセス要求元エンドエンティテイ（ユーザデバイス）制御部、

ＳＣ１：アクセス要求元ＥＥ内に構成されるセキュリティチップ、

アクセス先ＥＥ：アクセス要求先エンドエンティテイ（ユーザデバイス）制御部、

ＳＣ２：アクセス要求先ＥＥ内に構成されるセキュリティチップ、

である。

ここでは、アクセス元ＥＥ、アクセス先ＥＥはそれぞれ異なるユーザの通信処理装置である。また、セキュリティチップ（ＳＣ１，ＳＣ２）、ユーザセキュリティチップ（ＵＳＣ）は先に説明した図９のセキュリティチップと同様の構成を持ち、セキュリティチップにおいてグループ属性証明書の検証によるアクセス権限判定処理等が実行される。

すなわち、アクセス要求元デバイスからアクセス要求先に送付されたグループ属性証明書をネットワークインタフェース等の受信部で受信したアクセス要求先デバイスは、受信したグループ属性証明書をアクセス権限判定処理部としてのセキュリティチップに渡し、セキュリティチップ内で受信したグループ属性証明書に基づいて、アクセス権限判定処理が実行される。

なお、図２９以下の処理シーケンス図では、アクセス権限を有することを証明するグループ属性証明書の発行処理段階からの処理手続きについて説明する。すなわち、まず、通信処理装置のセキュリティチップがグループ属性証明書生成処理を実行し、アクセス権限を有することを証明するグループ属性証明書の発行処理を行なう。その後、発行されたグループ属性証明書を通信処理装置間で送受信してアクセス権限確認を行なう処理シーケンスである。従って、通信処理装置のセキュリティチップは、グループ属性証明書の生成手段、および検証手段として機能する。

図２９のシーケンス図に従って処理手順を説明する。まず、ステップＳ２０

１において、アクセス要求元のユーザがエンドエンティテイ（アクセス元ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）の新規発行要求コマンドを入力する。

エンドエンティテイ（アクセス元ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）の発行要求の入力を受領すると、ステップＳ２０２において、エンドエンティテイ（アクセス元ＥＥ）は、アクセス要求先のエンドエンティテイ（アクセス先ＥＥ）に対する接続要求を行ない、一方、ステップＳ２０３において、アクセス元エンドエンティテイ（アクセス元ＥＥ）内のセキュリティチップ（ＳＣ）に対して、相互認証開始要求を出力する。

ステップＳ２０４において、アクセス要求元のユーザデバイスのセキュリティチップ（ＳＣ１）と、アクセス要求先のエンドエンティテイ（アクセス先ＥＥ）に対応するセキュリティチップ（ＳＣ２）間の相互認証が実行される。これは例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ２０５では、アクセス要求元のセキュリティチップ（ＳＣ１）とユーザセキュリティチップ（ＵＳＣ）間の相互認証が実行され、ステップＳ２０６では、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）と、アクセス要求先のエンドエンティテイ（アクセス先ＥＥ）に対応するセキュリティチップ（ＳＣ２）間の相互認証が実行される。ステップＳ２０７では、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）からエンドエンティテイ（ＥＥ）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。

なお、ステップＳ２０５～Ｓ２０７の処理は、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）に対応するグループ属性証明書を発行する場合に必要となる処理であり、アクセス要求元のセキュリティチップ（ＳＣ１）に対応するグループ属性証明書を発行する場合には省略可能である。

上記各相互認証のいずれかが不成立の場合は、処理の続行は中止される。すべての相互認証が成立すると、ステップＳ２０８において、アクセス要求元のエンドエンティテイ（ＥＥ）は、アクセス要求先のセキュリティチップ（ＳＣ２）に対して、すでに保有済みのグループ属性証明書（Ｇｐ．ＡＣ）を提示し

て、新たなグループ属性証明書（Ｇｐ．ＡＣ）の発行要求を行なう。

ここでの処理は、アクセス要求元がすでに保有するグループ属性証明書（Ｇｐ．ＡＣ）を検証して新たな異なる定義のグループ属性証明書（Ｇｐ．ＡＣ）を発行する処理例である。すなわち新規発行のグループ属性証明書（Ｇｐ．ＡＣ）の発行ポリシーとして、既存のグループ属性証明書（Ｇｐ．ＡＣ）による属性の確認が含まれることになる。例えばユーザ本人であることの確認や、あるいは特定のメーカーの機器であることの確認を既存のグループ属性証明書（Ｇｐ．ＡＣ）に基づいて実行して、これらの確認がなされたことを条件として新規のグループ属性証明書（Ｇｐ．ＡＣ）の発行処理を行なうものである。

既存のグループ属性証明書（Ｇｐ．ＡＣ）の例としては、例えばユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）との相互認証を行なってユーザに対応して発行されるクレジットカード会社発行のグループ属性証明書がある。また、通信処理装置としての通信端末や、ＰＣ等エンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）との相互認証の結果としてエンドエンティテイ（ＥＥ）に格納されるメーカーの発行するメーカー製の端末であることを証明するグループ属性証明書等がある。

アクセス要求先デバイスのセキュリティチップ（ＳＣ２）は、アクセス要求元デバイスのエンドエンティテイ（ＥＥ）から受領した既発行のグループ属性証明書を検証する。この検証処理は、先に図２１～図２３を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。

アクセス要求先セキュリティチップ（ＳＣ２）は、検証結果をアクセス要求先エンドエンティテイ（ＥＥ）に出力し、検証不成功の場合は、エラー処理として、その後の処理を実行せず処理を中止する。この場合、エラー通知をアクセス要求元エンドエンティテイ（ＥＥ）に送信する処理を行なってもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ２１１に進む。ステップＳ２１１では、グループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、アクセス要求先エンドエンティテイ（ＥＥ）の保有するグループ情報データベース

に基づいて実行する。この審査処理は、先に図２５を参照して説明した処理と同様の処理である。すなわち、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）から発行者情報、グループ識別情報（グループＩＤ）を取得し、取得したＡＣ発行者、およびグループＩＤに基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

グループ属性証明書（Ｇｐ．ＡＣ）に対応するグループ情報が登録されていない場合、あるいはグループ情報の条件を満たさない場合は、審査不成功となり、エラーとして処理を中止する。一方、審査成功の場合はステップＳ２１２において、要求に従って、新たなグループ属性証明書の生成要求をセキュリティチップ（ＳＣ２）に出力し、セキュリティチップ（ＳＣ２）は、ステップＳ２１３において、要求に従って、グループ属性証明書を生成して、ステップＳ２１４において、アクセス先エンドエンティテイ（ＥＥ）からアクセス要求元ユーザデバイスのユーザ識別デバイス（ＵＩＤ）に対して新たなグループ属性証明書（Ｇｐ．ＡＣ）を発行する。

この新規発行グループ属性証明書は、例えば、アクセス要求先ユーザデバイスが会社Ｂのセキュアな情報を格納したＰＣ等の通信端末装置である場合、属性として、

「会社ＢからＵＩＤに発行された“会社Ｂの社員”という属性」

「会社ＢからＵＩＤに発行された“Ｃプロジェクトのメンバ”という属性」

等の属性に対応するものとなる。

会社Ｂのセキュアな情報を格納したＰＣ等の通信端末装置であるアクセス要求先ユーザデバイスは、不特定のユーザデバイスからのアクセス要求時に、グループ属性証明書の提示を要求して、提示されたグループ属性証明書の検証、審査を実行してアクセスの可否を決定することが可能となる。

次に、図３０を参照してアクセス許可情報を属性として持つグループ属性証明書の発行処理シーケンスについて説明する。図３０において、ステップＳ２２１～Ｓ２３５は、図２９におけるステップＳ２０１～Ｓ２１５に対応し、その処理も同様である。

図３０では、ステップＳ２２８において、アクセス要求元エンドエンティティ（アクセス元ＥＥ）がアクセス要求先ユーザデバイスのセキュリティチップ（ＳＣ２）に対して提示するグループ属性証明書が、「会社ＢからＵＩＤに発行された“会社Ｂの社員”という属性」を持つ証明書であり、アクセス要求先ユーザデバイスのセキュリティチップ（ＳＣ２）は、この属性証明書の検証、審査を実行して、新たなグループ属性証明書、すなわち、属性として、この機器（アクセス要求先ユーザデバイス）に対するアクセス可とした属性情報を持つ証明書を発行する構成である。

なお、この機器（アクセス要求先ユーザデバイス）に対するアクセス可としたグループ情報としての属性情報を持つ証明書を発行する条件として、「会社ＢからＵＩＤに発行された“会社Ｂの社員”という属性」を持つグループ属性証明書以外に、他のグループ属性証明書による証明が必要な場合は、ステップＳ２２８～Ｓ２３１の処理を必要なグループ属性証明書の数に対応する回数繰り返し実行する。

図３１を参照して、アクセス許可情報をグループ情報として持つグループ属性証明書と、他のグループ属性証明書との対応例について説明する。（ａ）は、アクセス許可情報をグループ情報として持つグループ属性証明書は、グループδに対応し、例えばこのグループδに対応するグループ属性証明書の発行条件は、グループαのメンバーであることが条件となる。例えばグループαのメンバーであることは、「会社ＢからＵＩＤに発行された“会社Ｂの社員”という属性」を証明するグループ属性証明書によって証明可能であり、グループδに対応するグループ属性証明書は、グループαのメンバーであることを証明するグループ属性証明書が提示され、その検証、審査が成功したことを条件として発行されることになる。

図３１（ｂ）は、アクセス許可情報をグループ情報として持つグループ属性証明書は、グループδに対応し、例えばこのグループδに対応するグループ属性証明書の発行条件は、グループαのメンバーであり、グループβのメンバーであり、グループγのメンバーであることすべての条件を満足することが条件となる。

具体的には、例えばユーザの居住地が特定の地域に属することを証明するグループ属性証明書α（グループα）と、ユーザ機器が特定メーカーの機器であることを示すグループ属性証明書β（グループβ）と、さらに、ユーザの年齢が所定の範囲に属することを示すグループ属性証明書γ（グループγ）の３つのグループ属性証明書の提示、検証によりグループδに対応するアクセス許可情報をグループ情報として持つグループ属性証明書を発行するといった設定である。

なお、アクセス要求元デバイスを構成する個人識別デバイスとしてのユーザ識別デバイスに対してグループ属性証明書を発行することにより、通信処理装置としてのエンドエンティテイ（ＥＥ）を変更した場合であっても、個人識別デバイスとしてのユーザ識別デバイスに対して発行したグループ属性証明書に基づく審査においてアクセスを許可することが可能となり、通信処理装置（エンドエンティテイ（ＥＥ））の変更によってアクセスが拒否されてしまうといったことを防止できる。

次に、図３２を参照して、アクセス要求先ユーザデバイスが、自ら属性証明書の発行処理を実行せずに属性証明書の発行処理を他のユーザデバイスに依頼して実行する処理シーケンスについて説明する。図３２において、

ＵＩＤ：アクセス要求元ユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：アクセス要求元ＵＩＤ内に構成されるユーザセキュリティチップ、

アクセス元ＥＥ：アクセス要求元エンドエンティテイ（ユーザデバイス）制御部、

ＳＣ１：アクセス要求元ＥＥ内に構成されるセキュリティチップ、

アクセス先ＥＥ：アクセス要求先エンドエンティテイ（ユーザデバイス）制御部、

ＳＣ２：アクセス要求先ＥＥ内に構成されるセキュリティチップ、

他ＥＥ：第３のユーザデバイス（手続き代行ユーザデバイス）

ＳＣ３：他ＥＥのセキュリティチップ、

である。

図３２において、ステップＳ２４１～Ｓ２４８は、図２９におけるステップＳ

２０１～Ｓ２０８に対応し、その処理も同様であり、説明を省略する。ステップＳ２４８において、アクセス要求先ユーザデバイスのエンドエンティティ（アクセス先ＥＥ）は、アクセス要求元エンドエンティティ（アクセス元ＥＥ）から提示されたグループ属性証明書を手続き代行ユーザデバイスのセキュリティチップ（ＳＣ３）に転送し、セキュリティチップ（ＳＣ３）が転送されたグループ属性証明書の検証（Ｓ２５０）を実行し、手続き代行ユーザデバイスのエンドエンティティ（他ＥＥ）が検証結果通知（Ｓ２５１）に基づいて、さらに審査（Ｓ２５２）を実行する。

さらに、検証、審査に成功したことを条件として、グループ属性証明書の生成要求をセキュリティチップ（ＳＣ３）に出力（Ｓ２５３）し、セキュリティチップ（ＳＣ３）は、ステップＳ２５４において、要求に従って、グループ属性証明書を生成して、ステップＳ２５５において、手続き代行エンドエンティティ（他ＥＥ）からアクセス要求元ユーザデバイスのユーザ識別デバイス（ＵＩＤ）に対して新たなグループ属性証明書（Ｇｐ．ＡＣ）を発行し、ステップＳ２５７においてアクセス要求元ユーザデバイスのユーザ識別デバイス（ＵＩＤ）が受領したグループ属性証明書を格納する。

図３２に示す処理シーケンスは、アクセス要求先ユーザデバイスが属性証明書の検証、審査、および発行機能を持たない場合に第３のデバイスにこれらの処理を委託して実行可能とした構成である。なお、手続き代行ユーザデバイスは、サービスプロバイダ（ＳＰ）等によって構成してもよい。

次に、アクセス許可情報をグループ情報として定義したグループ属性証明書を利用したアクセス可否判定処理を伴うサービス利用シーケンスについて、図３３を参照して説明する。

まず、ステップＳ２６１において、アクセス要求元のユーザがエンドエンティティ（アクセス元ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）の利用処理としてのアクセス要求コマンドを入力する。

エンドエンティティ（アクセス元ＥＥ）がユーザからの要求を受領すると、ステップＳ２６２において、エンドエンティティ（アクセス元ＥＥ）は、アクセス要求先のエンドエンティティ（アクセス先ＥＥ）に対する接続要求を行な

い、一方、ステップＳ２６３において、アクセス元エンドエンティテイ（アクセス元ＥＥ）内のセキュリティチップ（ＳＣ１）に対して、相互認証開始要求を出力する。

ステップＳ２６４において、アクセス要求元のユーザデバイスのセキュリティチップ（ＳＣ１）と、アクセス要求先のエンドエンティテイ（アクセス先ＥＥ）に対応するセキュリティチップ（ＳＣ２）間の相互認証が実行される。これは例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ２６５では、アクセス要求元のセキュリティチップ（ＳＣ１）とユーザセキュリティチップ（ＵＳＣ）間の相互認証が実行され、ステップＳ２６６では、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）と、アクセス要求先のエンドエンティテイ（アクセス先ＥＥ）に対応するセキュリティチップ（ＳＣ２）間の相互認証が実行される。ステップＳ２６７では、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）からエンドエンティテイ（ＥＥ）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。

なお、ステップＳ２６５～Ｓ２６７の処理は、アクセス要求元のユーザセキュリティチップ（ＵＳＣ）に対応するグループ属性証明書を利用した処理の場合に必要となる処理であり、アクセス要求元のセキュリティチップ（ＳＣ１）に対応するグループ属性証明書を利用した処理の場合には省略可能である。

上記各相互認証のいずれかが不成立の場合は、処理の続行は中止される。すべての相互認証が成立すると、ステップＳ２６８において、アクセス要求元のエンドエンティテイ（ＥＥ）は、アクセス要求先のセキュリティチップ（ＳＣ２）に対して、グループ属性証明書（Ｇｐ．ＡＣ）を提示して、アクセス許可を要求する。

アクセス要求先のセキュリティチップ（ＳＣ２）は、アクセス要求元のエンドエンティテイ（ＥＥ）から受領したグループ属性証明書を検証（Ｓ２６９）する。この検証処理は、先に図２１～図２３を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。

アクセス要求先セキュリティチップ（ＳＣ２）は、検証結果をアクセス要求先エンドエンティテイ（ＥＥ）に出力（Ｓ２７０）し、検証不成功の場合は、エラー処理として、その後の処理を実行せず処理を中止する。この場合、エラー通知をアクセス要求元エンドエンティテイ（ＥＥ）に送信する処理を行なってもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ２７１に進む。ステップＳ２７１では、グループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、アクセス要求先エンドエンティテイ（ＥＥ）の保有するグループ情報データベースに基づいて実行する。この審査処理は、先に図２５を参照して説明した処理と同様の処理である。すなわち、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）から発行者情報、グループＩＤを取得し、取得したＡＣ発行者、およびグループＩＤに基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。グループ情報には、例えば「この機器にアクセス可」、あるいは「データ読み出しのみ可」等の情報が含まれ、これらの情報に従ってサービスが提供される。

グループ属性証明書（Ｇｐ．ＡＣ）に対応するグループ情報が登録されていない場合、あるいはグループ情報の条件を満足しない場合は、審査不成功となり、エラーとして処理を中止する。一方、審査成功の場合はステップＳ２７２において、サービス提供、すなわち、グループ情報として登録されたサービス、例えば機器に対するアクセスを許可する。

［（５）グループ属性証明書の具体的利用例］

次に、グループ属性証明書の具体的利用例について説明する。以下、利用形態を、

（５－１）コンテンツ配信サービス

（５－２）リモートコントロールサービス

（５－３）リモートメンテナンスサービス

（５－４）パーソナルコミュニュケーションサービス

以上の各利用形態について各々説明する。

上記の各サービスにおいて利用されるグループ属性証明書の例を図３４に示す。図３４には、グループ属性証明書の発行者、発行タイミング、所有者、検証者、属性を対応付けて示してある。発行者は、前述したように、グループ属性証明書の発行処理のみを実行するグループＡＲＡの他、サービスプロバイダ、ユーザデバイス等、様々な発行主体が可能であり、サービスプロバイダとしては、例えばクレジットカードを発行する「カード会社Ａ」、所定の組織、例えば「会社Ｂ」、「役所」、さらにユーザ個人としての「甲さん」、さらにＰＣ、通信端末、ゲーム機等のエンドエンティテイ（ＥＥ）を製造する「ＥＥメーカーＣ」等がある。

グループ属性証明書の発行タイミングは、任意のタイミング、ＰＣ、通信端末、ゲーム機等のエンドエンティテイ（ＥＥ）の購入時、製造時、購入後等、証明書に基づいて提供するサービスに応じて、様々な設定が可能である。

グループ属性証明書の所有者は、所定のグループのメンバとしてのユーザ、あるいはユーザ機器であり、ユーザ、例えば「甲さん」を所有者として発行されるグループ属性証明書は、甲さんのユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）を対象としてユーザセキュリティチップ（ＵＳＣ）の認証に基づいて発行され、例えばある家族の各メンバに提供されるグループ属性証明書は、家族各々のユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）を対象としてユーザセキュリティチップ（ＵＳＣ）の認証に基づいて発行され、また、ＰＣ、通信端末、ゲーム機等のユーザ機器、すなわちエンドエンティテイ（ＥＥ）を対象として提供されるグループ属性証明書は、エンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）を対象としてユーザセキュリティチップ（ＵＳＣ）の認証に基づいて発行される。

これらのグループ属性証明書の検証処理の実行者は、グループ属性証明書によって証明される属性に基づいてサービスを提供するサービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）、あるいは図には示されていないが、ユーザデバイスのセキュリティチップ（ＳＣ，ＵＳＣ）である。

各グループ属性証明書の証明する所有者属性は、例えば「カード会社Ａ会員」、「会社Ｂの社員」、「甲さんの家族」、「登録されたユーザ」、「登録されたユーザデバイス」、「属性証明書発行者の所有機器（ＥＥ）」、「甲さんの所有機器（ＥＥ）」等であり、グループ属性証明書の検証、審査により、グループ属性証明書の提示ユーザまたは提示機器について、上記の各属性が証明されることになる。サービスプロバイダ等の属性証明書検証者は、証明された所有者属性に基づいて所定のサービスを提供する。

（５－１）コンテンツ配信サービス

まず、グループ属性証明書を利用したコンテンツ配信サービスについて説明する。コンテンツ配信におけるコンテンツの利用権限について、グループ属性証明書を適用して確認する態様としては、様々な態様がある。

まず、一例として、クレジットカード会社の発行するクレジットカード会員であることを証明する第１のグループ属性証明書Ａに基づいて、コンテンツの利用許可情報をグループ情報として含むコンテンツ配信サービス主体であるコンテンツ配信サービスプロバイダの発行する第２のグループ属性証明書Ｂの発行を行ない、この第２のグループ属性証明書Ｂを適用してコンテンツ利用権限の確認を実行してコンテンツ配信サービスを実行する処理例について説明する。

図３５を参照して、ユーザデバイスが、クレジットカード会員であることを証明する第１のグループ属性証明書Ａに基づいて、コンテンツの利用許可情報をグループ情報として含む第２のグループ属性証明書Ｂを発行する処理について説明する。

図３５の例においては、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）を対象として発行したクレジットカード会員であることを証明する第１のグループ属性証明書Ａをグループ属性証明書登録局（Ｇｐ．ＡＲＡ）に提示して、グループ属性認証局（Ｇｐ．ＡＡ）からコンテンツ配信サービスプロバイダが発行主体である第２のグループ属性証明書Ｂの発行処理例である。ここでは、コンテンツ配信サービスプロバイダは、グループ属性証

明書登録局（Ｇｐ．ＡＲＡ）と、グループ属性証明書発行ポリシーについて合意しているものとする。

図３５において、

ＵＩＤ：ユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：ＵＩＤ内に構成されるユーザセキュリティチップ、

ＥＥ：エンドエンティテイ（ユーザデバイス）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

グループＡＲＡ：グループ属性証明書登録局制御部、

グループＡＡ：グループ属性認証局制御部、

である。

まず、ステップＳ３０１において、ユーザがエンドエンティテイ（ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）の発行要求コマンドを入力する。この際、ユーザはグループ属性証明書発行に必要となる属性値を入力する。属性値は、グループＩＤ、あるいはグループに属することを証明する情報等である。

エンドエンティテイ（ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）の発行要求の入力を受領すると、ステップＳ３０２において、ユーザセキュリティチップ（ＵＳＣ）と、グループＡＲＡ間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにグループＡＲＡとの通信機能を持たないユーザ識別デバイス（ＵＩＤ）の場合は、

（１）ＥＥのＳＣとグループＡＲＡとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとグループＡＲＡとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

認証処理は、各デバイスのセキュリティチップの暗号処理部（図９参照）に

おける暗号処理を主とした処理によって実行され、例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ３０３では、ユーザセキュリティチップ（ＵＳＣ）からエンドエンティテイに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ３０４において、エンドエンティテイ（ＥＥ）は、グループＡＲＡに対してグループ属性証明書（Ｇｐ．ＡＣ）発行要求を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）発行要求には、エンドエンティテイ情報、属性値（例えばグループＩＤ、グループ情報）が含まれ、さらに、コンテンツ配信サービスプロバイダが発行主体である第２のグループ属性証明書Ｂの発行条件として提示すべき、クレジットカード会員であることを証明する第１のグループ属性証明書Ａが含まれる。

エンドエンティテイ（ＥＥ）からグループ属性証明書（Ｇｐ．ＡＣ）発行要求を受信したグループＡＲＡは、クレジットカード会員であることを証明する第１のグループ属性証明書Ａの検証の後、ステップＳ３０５において、発行ポリシーテーブルを参照して、ポリシーに準拠したグループ属性証明書の発行が可能か否かを判定し、可であれば、ステップＳ３０６に進み、不可であれば、発行不可メッセージをエンドエンティテイに通知する。

ステップＳ３０６では、グループＡＲＡが属性値（グループＩＤ）を伴うグループ属性証明書（Ｇｐ．ＡＣ）発行要求をグループＡＡに送信し、ステップＳ３０７において、グループＡＡが、グループＩＤを属性情報として格納し、電子署名を施したグループ属性証明書、すなわち、コンテンツの利用許可情報をグループ情報として含む第２のグループ属性証明書Ｂを生成し、グループＡＲＡに送信する。

ステップＳ３０８において、グループＡＲＡが、発行されたグループ属性証明書Ｂ（Ｇｐ．ＡＣ）をユーザ識別デバイス（ＵＩＤ）に送信する。ユーザ識別デバイス（ＵＩＤ）は、受信したグループ属性証明書（Ｇｐ．ＡＣ）をメモリに格納する。この際、グループ属性証明書（Ｇｐ．ＡＣ）の電子署名の検証を実行して、改竄の無いことを確認した後、メモリに格納する。

次に、図３６を参照して、上述の処理によって発行されたグループ属性証明書Ｂ、すなわちコンテンツの利用許可情報をグループ情報として含む第２のグループ属性証明書Ｂをサービスプロバイダに提示して、コンテンツ利用権限のあることの確認を行なって、サービス提供、すなわちコンテンツ配信サービスを受領する処理について説明する。図３６において、

ＵＩＤ：ユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：ＵＩＤ内に構成されるユーザセキュリティチップ、

ＥＥ：エンドエンティテイ（ユーザデバイス）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

ＳＰ：サービスプロバイダ制御部、

ＳＭ：ＳＰ内のセキュリティモジュール、

である。

セキュリティチップ（ＳＣ）、ユーザセキュリティチップ（ＵＳＣ）、セキュリティモジュール（ＳＭ）は先に説明した図９のセキュリティチップと同様の構成を持ち、セキュリティチップにおいてグループ属性証明書の検証による権限判定処理等が実行される。すなわち、サービス要求元デバイスからサービス要求先に送付されたグループ属性証明書をネットワークインタフェース等の受信部で受信したサービスプロバイダは、受信したグループ属性証明書を権限判定処理部としてのセキュリティモジュール（チップ）に渡し、セキュリティモジュール（チップ）内で受信したグループ属性証明書に基づいて、権限判定処理が実行される。

まず、ステップＳ３１１において、ユーザがエンドエンティテイ（ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）の利用要求コマンドを入力する。この際、ユーザは利用するグループ属性証明書に設定されたグループＩＤを指定する。ただし、特定のサービスを指定することにより唯一のグループＩＤが決定可能である場合は、サービスの指定のみとしてもよい。

エンドエンティテイ（ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）の利用要求入力を受領すると、ステップＳ３１２において、ユーザセキュ

リティチップ（ＵＳＣ）と、サービスプロバイダのセキュリティモジュール（ＳＭ）間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにＳＰとの通信を実行できないユーザ識別デバイス（ＵＩＤ）の場合は、

（１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部を中心として先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ３１３では、セキュリティチップからエンドエンティテイに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ３１４において、ユーザセキュリティチップ（ＵＳＣ）は、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対して自己のメモリに格納したグループ属性証明書（Ｇｐ．ＡＣ）を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）は、先に図３５を参照して説明した処理により取得したコンテンツの利用許可情報をグループ情報として含む第２のグループ属性証明書Ｂである。

ユーザセキュリティチップ（ＵＳＣ）からグループ属性証明書（Ｇｐ．ＡＣ）を受信したセキュリティモジュール（ＳＭ）は、ステップＳ３１５において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

グループ属性証明書（Ｇｐ．ＡＣ）の検証処理後、セキュリティモジュール

（ＳＭ）は、検証結果をサービスプロバイダ（ＳＰ）に出力し、検証不成立の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティティ通知する処理を実行してもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ３１７に進む。ステップＳ３１７では、先に図２５を参照して説明したグループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、サービスプロバイダの保有するグループ情報データベースに基づいて実行する。すなわち、サービスプロバイダ（ＳＰ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）から発行者情報、グループＩＤを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

この場合のグループ情報は、コンテンツの利用許可情報をグループ情報、例えばコンテンツとしてのゲームＸを３ヶ月利用可能とする情報等である。サービスプロバイダ（ＳＰ）は、ステップＳ３１８において、サービス提供処理、すなわち、グループ情報に従って、３ヶ月の利用期間を設定したゲームプログラムをユーザデバイスのエンドエンティティ（ＥＥ）に対して配信する。

上述したコンテンツ配信サービス処理は、１つのグループ属性証明書によってコンテンツ利用権の確認を行なう例であったが、次に、異なるグループ属性を証明する複数の異なる属性証明書を適用してユーザあるいはユーザ機器のコンテンツ利用権を確認してサービスを提供する処理例について説明する。

図３７に本処理例で適用する複数のグループ属性証明書を示す。グループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１は、Ａ大学によって発行され、Ａ大学の学生であることを証明する学生証であり、Ｃ君のユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）との認証に基づいて発行されたグループ属性証明書（Ｇｐ．ＡＣ）である。グループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２は、Ａ大学によって発行され、美術講座の受講権利を有することを証明する美術講座受講証であり、Ｃ君のユーザ識別デバイス（ＵＩＤ）のユーザセキュ

リティチップ(ＵＳＣ)との認証に基づいて発行されたグループ属性証明書(Ｇｐ．ＡＣ）である。

グループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０３は、Ａ大学によって発行され、Ａ大学の管理する機器であることを証明する管理機器証明書であり、エンドエンティテイ（ＥＥ）としてのテレビＤのセキュリティチップ（ＳＣ）との認証に基づいて発行されたグループ属性証明書（Ｇｐ．ＡＣ）である。グループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０４は、文部科学省によって発行され、教育使用目的の機器であることを証明する教育用機器証明書であり、エンドエンティテイ（ＥＥ）としてのテレビＤのセキュリティチップ（ＳＣ）との認証に基づいて発行されたグループ属性証明書（Ｇｐ．ＡＣ）である。

これらＡＣ０１～ＡＣ０４の４種類の異なるグループ属性証明書を適用したコンテンツ利用権限確認および、サービス提供処理について図３８を参照して説明する。

図３８は、ユーザデバイス側処理を左に、サービスプロバイダ側処理を右側に示している。なお、ユーザデバイスは、エンドエンティテイ（ＥＥ)、ＥＥ内に構成されるセキュリティチップ（ＳＣ)、ユーザ識別デバイス（ＵＩＤ)、ＵＩＤ内に構成されるユーザセキュリティチップ（ＵＳＣ）を含む。

ステップＳ３２１，Ｓ３３１において、ユーザデバイスと、サービスプロバイダ間の相互認証処理が実行される。なお、相互認証は、提示するグループ属性証明書の発行対象機に応じて実行し、ＥＥのＳＣとＳＰ－ＳＭとの相互認証、あるいは、ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証のいずれか、あるいはその双方が実行される。

本例の場合は、図３７に示す４つのグループ属性証明書中ＡＣ０１，ＡＣ０２は、Ｃ君のユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）を対象として発行されたものであり、ＡＣ０３，ＡＣ０４は、エンドエンティテイ（ＥＥ）としてのテレビＤに構成されるセキュリティチップ（ＳＣ）に対して発行されているものであるので、処理としては、Ｃ君のユーザ識別デバイス（ＵＩＤ）をエンドエンティテイ（ＥＥ）としてのテレビＤに接続機器インタフェース２３１（図９参照）を介して接続し、エンドエンティテイ（Ｅ

E）としてのテレビDのネットワークインタフェース２３２（図９参照）を介してサービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）と接続し、ＥＥのＳＣとＳＰ－ＳＭとの相互認証、および、ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証の双方を実行する。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ３２２において、ユーザデバイスは、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対して自己のメモリに格納した複数のグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１～ＡＣ０４を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１～ＡＣ０４は、図３７に示す４種類のグループ属性証明書である。

なお、サービス提供にあたり、必要となるグループ属性証明書の組み合わせデータは、サービスプロバイダ側からユーザ側に通知する構成としてもよい。サービスプロバイダは、例えば図３９に示すサービス提供条件として設定されるグループ属性証明書の組み合わせテーブルデータを保有する。図３９に示す例では、例えばサービスとしてコンテンツＢの視聴のためには、Ａ大学発行の学生証としてのグループ属性証明書、文部科学省発行の教育用機器証明書としてのグループ属性証明書等が必要であることを示すデータが格納され、このテーブルを適用して、必要となるグループ属性証明書の提示をユーザデバイスに対して通知する。

ステップＳ３３２において、ユーザデバイスから本例におけるサービス提供に必要となる４種類のグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１～ＡＣ０４を受信したセキュリティモジュール（ＳＭ）は、ステップＳ３３３において、複数のグループ属性証明書から、順次１つのグループ属性証明書を選択し、検証処理を実行する。グループ属性証明書の検証処理については、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

グループ属性証明書（Ｇｐ．ＡＣ）の検証処理後、検証不成立（Ｓ３３４：Ｎｏ）の場合は、エラー処理（Ｓ３３９）として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティテイ通知する処理を実行してもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成立（Ｓ３３４：Ｙｅｓ）し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ３３５に進む。ステップＳ３３５では、先に図２５を参照して説明したグループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、サービスプロバイダの保有するグループ情報データベースに基づいて実行する。すなわち、サービスプロバイダ（ＳＰ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）から発行者情報、グループＩＤを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。この場合のグループ情報は、コンテンツの配信許可情報を含む情報である。

グループ属性証明書の審査が不成立（Ｓ３３６：Ｎｏ）の場合、例えば、グループ情報の取得に失敗した場合は、エラー処理（Ｓ３３９）として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティテイ通知する処理を実行してもよい。

グループ属性証明書の審査が成立（Ｓ３３６：Ｙｅｓ）した場合、ステップＳ３３７に進み、提示されたグループ属性証明書の全ての検証、審査が終了したか否かを判定し、未終了分がある場合は、ステップＳ３３３以下の検証、審査処理を未終了分のグループ属性証明書について実行する。

ステップＳ３３７において、提示されたグループ属性証明書の全ての検証、審査が終了したと判定した場合は、ステップＳ３３８において、サービス提供を実行し、ユーザデバイスにおいてステップＳ３４０のサービス受領を実行する。具体的には、エンドエンティテイとしてのテレビＤ（図３７参照）において、ユーサＣ君が配信コンテンツの視聴を可能となる。

上述した複数のグループ属性証明書を適用した利用権限確認処理を模式図で示すと、図４０のように示される。すなわち、４種類の異なる属性を定義し

たグループ属性証明書の定義領域が、図４０に示すグループＡＣ０１～ＡＣ０４によって示されるとき、上述したコンテンツの利用権限が認められるためには、（ａ）に示すように、ユーザのグループ属性としての学生証（グループ属性証明書（ＡＣ０１）と美術講座受講証（ＡＣ０２）の両グループに属していること、および利用機器のグループ属性として、（ｂ）に示すように、機器のグループ属性として、管理機器証明書と、教育機器証明書を保有する機器であることの両条件を満足することが必要となる。

（ａ）に示すユーザのグループ属性としての学生証（グループ属性証明書（ＡＣ０１）と美術講座受講証（ＡＣ０２）の両グループに属していることの証明は、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）対応のグループ属性証明書の検証、審査によって確認され、（ｂ）に示す機器のグループ属性としての管理機器証明書と、教育機器証明書を保有する機器であることの証明はエンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）対応のグループ属性証明書の検証、審査によって確認される。

なお、図３９を参照して説明したフローにおいては、４つのグループ属性証明書の検証、審査が成功したことを条件としてサービスを提供する処理としたが、４つのグループ属性証明書の検証、審査が成功したことを条件としてサービスを実行するのではなく、サービス提供を認める新たなグループ属性証明書を発行する処理を行ない、ユーザが新たにこの１つの新規発行のグループ属性証明書を提示し、その検証を実行することによりサービスの提供を受けることが可能となる。

ただし、この場合、この新規発行されたグループ属性証明書は、ユーザグループおよび機器グループの両グループを定義するものとなり、グループ定義に合致するユーザ識別デバイス（ＵＩＤ）をグループ定義に合致する機器（ＥＥ）に設定し、ＵＩＤのセキュリティチップ（ＵＳＣ）とサービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）との相互認証により、ＵＩＤのセキュリティチップ（ＵＳＣ）認証が成立し、さらに、エンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）とサービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）との相互認証によりセキュリティチップ（ＳＣ）の認証が

成立し、さらに、上述の新規発行グループ属性証明書の検証、審査が成立することがサービス利用条件となる。

（５－２）リモートコントロールサービス

次に、グループ属性証明書に基づく、データ処理システム構成の一例として権限確認を実行してエンドエンティティ（ＥＥ）としての機器のリモートコントロールを実行するサービス利用例について説明する。

ここでは、医療機器をエンドエンティティ（ＥＥ）として、自宅等に設置した医療機器と、サービスプロバイダとしての病院側の医療機器（ＳＰ）との間で通信を実行して、病院側の医療機器（ＳＰ）から送信する命令に基づいて、自宅設置の医療機器（ＥＥ）によりユーザの医療診断、検査等を実行し、検査データ等の取得情報を自宅設置の医療機器（ＥＥ）から病院側の医療機器（ＳＰ）に送信する医療処理例について説明する。

上述の医療処理を実行するデータ処理システムにおける各処理の実行の際、それぞれグループ属性証明書の検証、審査に基づいて処理の実行可否を確認する処理が行なわれ、実行可否確認の後、医療処理手続きに係る様々なデータ処理が実行される。適用するグループ属性証明書の例を図４１に示す。

グループ属性証明書ＡＣ０１は、発行者が、サービスプロバイダ（ＳＰ）としての病院側医療機器であり、所有者、すなわちグループ属性証明書ＡＣ０１の発行時に発行者である病院側医療機器（ＳＰ）と認証処理を行なうことによりグループ属性証明書の発行対象となった所有者は、自宅側医療機器（ＥＥ）によって医療サービスを受けるユーザ甲さんのユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）である。あるいは自宅側医療機器（ＥＥ）のセキュリティチップ（ＳＣ）であってもよい。

このグループ属性証明書ＡＣ０１は、医療プログラムの実行可否を判定する確認処理の際に適用され、所有者であるユーザデバイスのＵＳＣあるいはＳＣから病院側医療機器（ＳＰ）に送付されて、病院側医療機器（ＳＰ）において、グループ属性証明書ＡＣ０１の検証、審査の後、サービス、すなわち医療診断プログラムの実行が許可される。

グループ属性証明書ＡＣ０２は、発行者が、自宅側医療機器（ＥＥ）であり、所有者、すなわちグループ属性証明書ＡＣ０２の発行時に発行者である自宅側医療機器（ＥＥ）と認証処理を行なうことによりグループ属性証明書の発行対象となった所有者は、サービスプロバイダ（ＳＰ）としての病院側医療機器のセキュリティモジュール（ＳＭ）である。

このグループ属性証明書ＡＣ０２は、医療プログラムの実行によって診断対象者（甲さん）から取得し、診断データ、例えば血圧値、脈拍、採血データ等の診断データを、自宅側医療機器（ＥＥ）から病院側医療機器（ＳＰ）に対して送信する処理の実行可否判定処理に適用される。

このグループ属性証明書ＡＣ０２は、病院側医療機器（ＳＰ）から自宅側医療機器（ＥＥ）に送付されて、自宅側医療機器（ＥＥ）において、グループ属性証明書ＡＣ０２の検証、審査の後、サービス、すなわち医療診断結果データの送付処理が実行される。

なお、グループ属性証明書ＡＣ０１，ＡＣ０２の発行処理は、病院側医療機器（ＳＰ）あるいは自宅側医療機器（ＥＥ）、あるいはユーザ識別デバイス（ＵＩＤ）自体が、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）の機能を実行して、みずから発行することが可能であるが、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）に依頼して発行処理を行なう構成も可能である。ただし、この場合には発行者のポリシーに従った処理が実行されることが条件である。

例えばグループ属性証明書ＡＣ０１の発行処理は、発行者である病院側医療機器（ＳＰ）あるいは、発行代理を行なうグループ属性証明書登録局（グループＡＲＡ）が、医療診断対象者としての甲さんから、甲さんであることを証明する既発行のグループ属性証明書、例えばクレジットカード会社の発行したグループ属性証明書を提示させ、その提出されたグループ属性証明書の検証を実行した後、新たなグループ属性証明書ＡＣ０１の発行処理を行なう方法をとることが好ましい。このような既発行のグループ属性証明書の検証を条件として、新たなグループ属性証明書を発行する処理シーケンスは、先に図２９、図３０、

図３２等を参照して説明した処理シーケンスと同様となる。

また、グループ属性証明書ＡＣ０２の発行処理においても、同様に、発行者である自宅側医療機器（ＥＥ）あるいは、発行代理を行なうグループ属性証明書登録局（グループＡＲＡ）が、病院側医療機器（ＳＰ）から、病院側医療機器（ＳＰ）であることを証明する既発行のグループ属性証明書、例えばメーカーあるいは公の管理組織の発行したグループ属性証明書を提示させて、その提出されたグループ属性証明書の検証を実行した後、グループ属性証明書ＡＣ０２の発行処理を行なう方法をとることが好ましい。

医療処理を行なうリモートコントロールのシステムにおいて、各機器に格納される属性証明書は、図４２に示す通りとなる。サービスプロバイダとしての病院側医療機器（ＳＰ）４０１と、エンドエンティテイとしての自宅側医療機器（ＥＥ）４１１は通信ネットワークにより相互にデータ転送可能であり、自宅側医療機器（ＥＥ）４１１と、ユーザ識別デバイス（ＵＩＤ）４２１は、双方の接続機器インタフェース２３１（図９参照）を介して相互にデータ転送が可能である。

それぞれの機器には、耐タンパ構成を持つ（ユーザ）セキュリティチップ４１２，４２３またはセキュリティモジュール４０３が備えられ、データ通信処理の際の相互認証処理、あるいは転送データの暗号化、復号処理等を実行する。またグループ属性証明書の検証処理も（ユーザ）セキュリティチップ４１２，４２３またはセキュリティモジュールにおいて実行される。

ユーザ識別デバイス４２１には、先に図４１を参照して説明したグループ属性証明書ＡＣ０１，４２２が格納される。グループ属性証明書ＡＣ０１，４２２は、発行者が、サービスプロバイダとしての病院側医療機器（ＳＰ）４０１であり、医療プログラムの実行可否を判定する確認処理の際に適用され、所有者であるユーザデバイスのＵＳＣ４２１から病院側医療機器（ＳＰ）４０１に送付されて、病院側医療機器（ＳＰ）４０１のセキュリティモジュール（ＳＭ）４０３において、グループ属性証明書ＡＣ０１の検証、審査の後、サービス、すなわち医療診断プログラムが実行される。

また、サービスプロバイダとしての病院側医療機器（ＳＰ）４０１には、グ

ループ属性証明書ＡＣ０２，４０２が格納される。グループ属性証明書ＡＣ０２，４０２は、発行者が、自宅側医療機器（ＥＥ）４１１であり、所有者が病院側医療機器（ＳＰ）４０１であり、病院側医療機器（ＳＰ）から自宅側医療機器（ＥＥ）に送付され、診断対象者（甲さん）から取得した診断データを、自宅側医療機器（ＥＥ）４１１から病院側医療機器（ＳＰ）４０１に対する送信処理の前に、自宅側医療機器（ＥＥ）４１１のセキュリティチップ（ＳＣ）４１２においてグループ属性証明書ＡＣ０２，４０２の検証、審査が実行され、検証、審査成立を条件として診断結果データの送信が実行される。

図４３を参照して、ユーザ識別デバイス４２１に格納されたグループ属性証明書ＡＣ０１，４２２を適用して医療診断プログラムの実行サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する。図４３において、

ＵＩＤ：ユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：ＵＩＤ内に構成されるユーザセキュリティチップ、

ＥＥ：自宅側医療機器（ＥＥ）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

ＳＰ：病院側医療機器（ＳＰ）制御部、

ＳＭ：ＳＰ内のセキュリティモジュール、

である。

セキュリティチップ（ＳＣ）、ユーザセキュリティチップ（ＵＳＣ）、セキュリティモジュール（ＳＭ）は先に説明した図９のセキュリティチップと同様の構成を持ち、セキュリティモジュールまたはチップにおいてグループ属性証明書の検証による権限判定処理等が実行される。すなわち、サービス、ここではデータ処理要求元デバイスからデータ処理要求先に送付されたグループ属性証明書をネットワークインタフェース等の受信部で受信したサービスプロバイダまたはユーザデバイスは、受信したグループ属性証明書を権限判定処理部としてのセキュリティモジュール（チップ）に渡し、セキュリティモジュール（チップ）内で受信したグループ属性証明書に基づいて、権限判定処理が実行し、権限ありの判定に基づいて、様々なデータ処理を実行する。

まず、ステップＳ３２１において、ユーザがエンドエンティテイとしての自宅側医療機器（ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）＝ＡＣ０１の利用要求コマンドを入力する。このグループ属性証明書（Ｇｐ．ＡＣ）は、図４１、図４２に示すＡＣ０１である。この処理の際、ユーザは利用するグループ属性証明書ＡＣ０１に設定されたグループＩＤを指定する。ただし、特定のサービスを指定することにより唯一のグループＩＤが決定可能である場合は、サービスの指定のみとしてもよい。

自宅側医療機器（ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１の利用要求入力を受領すると、ステップＳ３２２において、ユーザセキュリティチップ（ＵＳＣ）と、サービスプロバイダとしての病院側医療機器（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにＳＰとの通信を実行できないユーザ識別デバイス（ＵＩＤ）の場合は、

（１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ３２３では、ユーザセキュリティチップからエンドエンティテイに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ３２４において、ユーザセキュリティチップ（ＵＳＣ）は、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対して自己のメモリに格納したグループ属性証明

書（Ｇｐ．ＡＣ）ＡＣ０１を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）は、先に図４１、図４２を参照して説明したように、医療プログラムのサービス受領資格権限を判定する処理に適用するグループ属性証明書ＡＣ０１である。

ユーザセキュリティチップ（ＵＳＣ）からグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１を受信した病院側医療機器（ＳＰ）のセキュリティモジュール（ＳＭ）は、ステップＳ３２５において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

グループ属性証明書（Ｇｐ．ＡＣ）の検証処理後、セキュリティモジュール（ＳＭ）は、検証結果を病院側医療機器（ＳＰ）に出力し、検証不成立の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティテイ通知する処理を実行してもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ３２７に進む。ステップＳ３２７では、先に図２５を参照して説明したグループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、サービスプロバイダとしての病院側医療機器（ＳＰ）の保有するグループ情報データベースに基づいて実行する。すなわち、病院側医療機器（ＳＰ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１から発行者情報、グループＩＤを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

この場合のグループ情報は、医療診断プログラムの実行許可情報を含むものである。サービスプロバイダとしての病院側医療機器（ＳＰ）は、ステップＳ３２８において、サービス提供処理、すなわち、グループ情報に従って、医療診断プログラムの実行を行なう。すなわち、リモートコントロールによる医療

診断処理、すなわち各種診断プログラムの実行コマンドを自宅側医療機器（ＥＥ）に送信して自宅側医療機器（ＥＥ）を介してユーザの診断を実行する。

次に、図４４を参照して、病院側医療機器（ＳＰ）４０１に格納されたグループ属性証明書ＡＣ０２，４０２を適用して医療診断プログラムの実行結果としての診断データ引き取り処理サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する。

まず、ステップＳ３３１において、病院側のシステムを操作するユーザが病院側医療機器（ＳＰ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）＝ＡＣ０２の利用要求コマンドを入力する。このグループ属性証明書（Ｇｐ．ＡＣ）は、図４１、図４２に示すＡＣ０２である。この処理の際、病院側のシステムを操作するユーザは利用するグループ属性証明書ＡＣ０２に設定されたグループＩＤを指定する。ただし、特定のサービスを指定することにより唯一のグループＩＤが決定可能である場合は、サービスの指定のみとしてもよい。

病院側医療機器（ＳＰ）がグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２の利用要求入力を受領すると、ステップＳ３３２において、ユーザセキュリティチップ（ＵＳＣ）と、サービスプロバイダとしての病院側医療機器（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにＳＰとの通信を実行できないユーザ識別デバイス（ＵＩＤ）の場合は、

（１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図

９参照)を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ３３３では、セキュリティモジュール（ＳＭ）から病院側医療機器（ＳＰ）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ３３４において、病院側医療機器（ＳＰ）のセキュリティモジュール（ＳＭ）は、自宅側医療機器側のユーザセキュリティチップ（ＵＳＣ）に対して自己のメモリに格納したグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）は、先に図４１、図４２を参照して説明したように、診断結果データの引き取り処理権限を判定する処理に適用するグループ属性証明書ＡＣ０２である。

病院側医療機器（ＳＰ）のセキュリティモジュール（ＳＭ）からグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２を受信したユーザセキュリティチップ（ＵＳＣ)は、ステップＳ３３５において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

グループ属性証明書（Ｇｐ．ＡＣ）の検証処理後、ユーザセキュリティチップ（ＵＳＣ）は、検証結果を自宅側医療機器（ＥＥ）に出力（Ｓ３３６）し、検証不成立の場合は、エラー処理として、診断結果の送信サービスを実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨を病院側医療機器（ＳＰ）に通知する処理を実行してもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ３３７に進む。ステップＳ３３７では、先に図２５を参照して説明したグループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、自宅側医療機器（ＥＥ）の保有するグループ情報データベースに基づいて実行する。すなわち、自宅側医療機器（ＥＥ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２から発行者情報、グループＩＤを取得し、取得情報に基づいて、グループ情報データベースを検索し、登

録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

この場合のグループ情報は、医療診断プログラムの診断結果送信許可情報を含むものである。自宅側医療機器（ＥＥ）は、ステップＳ３３８において、サービス提供処理、すなわち、グループ情報に従って、医療診断プログラムの診断結果送信処理を実行する。すなわち、医療診断処理結果を自宅側医療機器（ＥＥ）から病院側医療機器（ＳＰ）に送信する処理を実行する。

（５－３）リモートメンテナンスサービス

次に、グループ属性証明書に基づいて権限確認を実行してデータ処理の実行を行なうデータ処理システムの構成例として、エンドエンティテイ（ＥＥ）としての機器、例えば家電製品のリモートメンテナンスを実行するサービス利用例について説明する。

ここでは、通信機能を有するＡＶ機器、エアコン、冷蔵庫等の様々な家電機器をエンドエンティテイ（ＥＥ）として、自宅等に設置したこれらの家電機器と、サービスプロバイダとしての家電機器メーカー側のサービス提供機器（ＳＰ）との間で通信を実行して、メーカー側のサービス提供機器（ＳＰ）から送信する命令に基づいて、自宅設置の家電機器（ＥＥ）の修理、メンテナンス、アップグレード、その他コントロール処理を実行する例について説明する。

上述の各処理の実行の際、それぞれグループ属性証明書の検証、審査に基づいて処理の実行可否を確認する処理が行なわれ、実行可否確認の後、各処理が実行される。適用するグループ属性証明書の例を図４５に示す。グループ属性証明書は、大きく２つのカテゴリに分類される。１つはサービス属性証明書（ＡＣ）であり、他方はコントロール属性証明書（ＡＣ）である。

サービス属性証明書（ＡＣ）は、発行者が、サービスプロバイダ（ＳＰ）としての家電機器メーカー側機器であり、所有者、すなわちサービス属性証明書（ＡＣ）の発行時に発行者である家電機器メーカー側機器（ＳＰ）と認証処理を行なうことにより属性証明書の発行対象となった所有者は、自宅等に設置した家電機器（ＥＥ）を利用するユーザのユーザ識別デバイス（ＵＩＤ）のユー

ザセキュリティチップ（ＵＳＣ）、あるいは家電機器（ＥＥ）のセキュリティチップ（ＳＣ）である。

このサービス属性証明書は、家電機器を購入したユーザとメーカー側との間で、家電機器購入時にサブスクライバ契約を交わすことで、その後の家電機器（ＥＥ）の修理、メンテナンス、アップグレード、その他コントロール処理に関するサービスを受領する権限を認めた家電機器購入者グループ、あるいは家電機器グループに対して発行されるものである。従って、サービス属性証明書は、家電機器購入者グループ、あるいは家電機器グループを対象として発行されるグループ属性証明書である。

家電機器購入者グループを対象として発行する場合は、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）と家電機器メーカー（ＳＰ）のセキュリティモジュール間の相互認証の成立を条件とした発行処理がなされ、家電機器グループを対象として発行する場合は、家電機器（ＥＥ）のセキュリティチップ（ＳＣ）と家電機器メーカー（ＳＰ）のセキュリティモジュール間の相互認証の成立を条件とした発行処理がなされる。

このサービス属性証明書は、家電機器（ＥＥ）の修理、メンテナンス、アップグレード、その他コントロールサービスの要求の際に、家電機器（ＥＥ）あるいはユーザ識別デバイス（ＵＩＤ）からメーカー側機器（ＳＰ）に送付されて、メーカー側機器（ＳＰ）において、サービス属性証明書の検証、審査の後、サービスの提供に移行することになる。

コントロール属性証明書は、発行者が、修理、メンテナンス、アップグレード、その他コントロールサービスを受領する家電機器（ＥＥ）であり、所有者、すなわちコントロール属性証明書の発行時に発行者である家電機器（ＥＥ）と認証処理を行なうことによりグループ属性証明書の発行対象となった所有者は、サービスプロバイダ（ＳＰ）としてのメーカー側機器のセキュリティモジュール（ＳＭ）である。

このコントロール属性証明書は、家電機器を購入したユーザとメーカー側との間で、家電機器購入以後に、サービス属性証明書の保有を条件として発行される証明書であり、例えば同一メーカーの複数の家電機器を有するユーザーが、

各々の家電機器に対するメンテナンスサービス実行範囲を権限情報とした証明書として、各家電機器に対応して、サービス提供者であるメーカー側機器に対して発行する。あるいは、１つの家電機器に対して、異なるコントロール権限情報を各々記録した証明書として発行することも可能である。例えば、家電機器のコントロール情報として、ソフトウェアのアップグレード処理依頼のために、アップグレード処理のみを受領サービスとして許容することを示す属性証明書、あるいは、定期点検のための点検処理のみを許容することを示す属性証明書等である。

コントロール属性証明書は、例えば１ユーザの所有する複数の家電機器グループ、あるいは１つの家電機器を対象として複数発行可能なグループ属性証明書である。１ユーザの所有する複数の家電機器グループを対象として発行する場合は、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）と家電機器メーカー（ＳＰ）のセキュリティモジュール間の相互認証の成立を条件とした発行処理がなされ、１つの特定の家電機器を対象として発行する場合は、上述のＵＩＤのＵＳＣ、あるいは特定の家電機器（ＥＥ）のセキュリティチップ（ＳＣ）と家電機器メーカー（ＳＰ）のセキュリティモジュール間の相互認証の成立を条件とした発行処理がなされる。

このコントロール属性証明書は、ユーザ側（ＥＥまたはＵＩＤ）から発行されてサービスを提供するメーカー側機器に格納され、家電機器（ＥＥ）の修理、メンテナンス、アップグレード、その他コントロールサービスの実行時にメーカー側機器から、ユーザ側（ＥＥまたはＵＩＤ）に送信されて、ユーザ側（ＥＥまたはＵＩＤ）において、コントロール属性証明書の検証、審査の後、サービスの提供に移行することになる。

なお、サービス属性証明書、コントロール属性証明書の発行処理は、メーカー側機器（ＳＰ）あるいは家電機器（ＥＥ）、あるいはユーザ識別デバイス（ＵＩＤ）自体が、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）の機能を実行して、みずから発行することが可能であるが、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）に依頼して発行処理を行なう構成も可能である。ただ

し、この場合には発行者のポリシーに従った処理が実行されることが条件である。

例えばサービス属性証明書の発行処理は、発行者であるメーカー側機器（ＳＰ）あるいは、発行代理を行なうグループ属性証明書登録局（グループＡＲＡ）が、サービス提供を受けようとするユーザから、ユーザ自身を証明する既発行のグループ属性証明書、例えばクレジットカード会社の発行したグループ属性証明書を提示させ、その提出されたグループ属性証明書の検証を実行した後、新たなグループ属性証明書として、サービス属性証明書を発行したり、あるいは家電機器に対して、製造時にメーカーが格納したメーカー製の製品グループに属することを証明するグループ属性証明書を提示させ、その提出されたグループ属性証明書の検証を実行した後、新たなグループ属性証明書として、サービス属性証明書を発行するといった発行処理を行なうことが好ましい。このような既発行のグループ属性証明書の検証を条件として、新たなグループ属性証明書を発行する処理シーケンスは、先に図２９、図３０、図３２等を参照して説明した処理シーケンスと同様となる。

また、コントロール属性証明書の発行処理においても、同様に、発行者である家電機器（ＥＥ）あるいは、発行代理を行なうグループ属性証明書登録局（グループＡＲＡ）が、メーカー側機器（ＳＰ）から、メーカー側の真正な機器であることを証明する既発行のグループ属性証明書、例えば、前述したようにメーカーの発行したグループ属性証明書としてのサービス属性証明書を提示させて、その提出証明書の検証を実行した後、新たなグループ属性証明書としてのコントロール属性証明書の発行処理を行なう方法をとることが好ましい。

メンテナンスサービスを行なうシステムにおいて、各機器に格納される属性証明書は、図４６に示す通りとなる。サービスプロバイダとしてのメーカー側機器（ＳＰ）４５１と、エンドエンティテイとしてのユーザー側家電療機器（ＥＥ）４６１は通信ネットワークにより相互にデータ転送可能であり、ユーザー側家電機器（ＥＥ）４６１と、ユーザ識別デバイス（ＵＩＤ）４７１は、双方の接続機器インタフェース２３１（図９参照）を介して相互にデータ転送が可能である。

それぞれの機器には、耐タンパ構成を持つ（ユーザ）セキュリティチップ４６３，４７２またはセキュリティモジュール４５３が備えられ、データ通信処理の際の相互認証処理、あるいは転送データの暗号化、復号処理等を実行する。またグループ属性証明書の検証処理も（ユーザ）セキュリティチップ４６３，４７２またはセキュリティモジュール４５３において実行される。

ユーザ側家電機器（ＥＥ）４６１には、先に図４５を参照して説明したサービス属性証明書４６２が格納される。サービス属性証明書４６２は、発行者が、サービスプロバイダとしてのメーカー側機器（ＳＰ）４５１であり、家電メンテナンス、修理等の実行可否を判定する確認処理の際に適用され、所有者であるユーザ側家電機器（ＥＥ）４６１のＳＣ４６３からメーカー側機器（ＳＰ）４５１に送付される。メーカー側機器（ＳＰ）４５１のセキュリティモジュール（ＳＭ）４５３において検証、審査の後、サービス、すなわちコントロール属性証明書送信、およびコントロール属性証明書によって許可された権限範囲でのメンテナンス等の処理が実行される。

サービスプロバイダとしてのメーカー側機器（ＳＰ）４５１には、コントロール属性証明書４５２が格納される。コントロール属性証明書４５２は、発行者が、ユーザ側家電機器（ＥＥ）４６１であり、所有者がメーカー側機器（ＳＰ）４５１であり、メーカー側機器（ＳＰ）からユーザー側家電機器（ＥＥ）４６１に送付され、メンテナンス等のサービス実行の前に、ユーザー側家電機器（ＥＥ）４６１のセキュリティチップ（ＳＣ）４６３においてコントロール属性証明書の検証、審査が実行され、検証、審査成立を条件としてメンテナンス、修理、あるいはアップグレード等の処理が、コントロール属性証明書によって確認された権限範囲内で実行される。

サービス実行時におけるサービス属性証明書およびコントロール属性証明書の利用形態について、図４７を参照して説明する。まず、メンテナンス、修理、点検、アップグレード等のサービスを受領したい家電機器（ＥＥ）あるいは家電機器に接続したユーザ識別デバイス（ＵＩＤ）側から、サービス属性証明書（ＡＣ）４８４をメーカー側機器（ＳＰ）４８２に提示する。メーカー側機器（ＳＰ）４８２は、セキュリティモジュール（ＳＭ）におけるサービス属

性証明書の検証の後、サービス属性証明書に対応するグループＩＤに基づいて、グループ情報データベース４８３を検索して、グループ情報としてのコントロールＡＣあるいはコントロールＡＣの識別データを抽出して、サービスＡＣに対応するコントロールＡＣを取得する。

メーカー側機器（ＳＰ）４８２は、取得したコントロール属性証明書（ＡＣ）４８５を家電機器（ＥＥ）あるいは家電機器に接続したユーザ識別デバイス（ＵＩＤ）に送信し、家電機器（ＥＥ）あるいは家電機器に接続したユーザ識別デバイス（ＵＩＤ）におけるセキュリティチップで検証の後、コントロール属性証明書（ＡＣ）で許容されたコントロール情報に従って家電機器（ＥＥ）に対してメンテナンス等のサービスが実行される。

なお、メンテナンス、修理、アップグレード等の実行プログラムは、予め家電機器内のメモリに格納したものを利用してもよく、あるいは、必要に応じて、メーカー側機器から家電機器に対して送信して実行する構成としてもよい。なお、実行プログラムの送信の際には、認証処理、送信データの暗号化処理を実行することが好ましい。

次に、図４８以下を参照して、ユーザデバイスとしての家電機器（ＥＥ）に格納されたサービス属性証明書、サービスプロバイダに格納されたコントロール属性証明書を適用して家電機器のメンテナンス等のサービスに関する利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する。

図４８において、

ＥＥ：ユーザ側家電機器（ＥＥ）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

ＳＰ：メーカー側機器（ＳＰ）制御部、

ＳＭ：ＳＰ内のセキュリティモジュール、

である。

セキュリティチップ（ＳＣ）、ユーザセキュリティチップ（ＵＳＣ）、セキュリティモジュール（ＳＭ）は先に説明した図９のセキュリティチップと同様の構成を持ち、セキュリティモジュールまたはチップにおいてグループ属性証明書の検証による権限判定処理等が実行される。すなわち、サービス、ここでは

メンテナンス処理等のデータ処理要求元デバイスからデータ処理要求先に送付されたグループ属性証明書をネットワークインタフェース等の受信部で受信したサービスプロバイダまたはユーザデバイスは、受信したグループ属性証明書を権限判定処理部としてのセキュリティモジュール（チップ）に渡し、セキュリティモジュール(チップ)内で受信したグループ属性証明書に基づいて、権限判定処理が実行し、権限ありの判定に基づいて、様々なデータ処理を実行する。

まず、ステップＳ３４１において、ユーザがエンドエンティテイとしてのユーザ側家電機器（ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）であるサービス属性証明書（ＡＣ）の利用要求コマンドを入力する。この処理の際、ユーザは利用するサービス属性証明書（ＡＣ）に設定されたグループＩＤを指定する。ただし、特定のサービスを指定することにより唯一のグループＩＤが決定可能である場合は、サービスの指定のみとしてもよい。

ユーザ側家電機器（ＥＥ）がユーザからのサービス属性証明書（ＡＣ）の利用要求入力を受領すると、ステップＳ３４２において、セキュリティチップ(ＳＣ）と、サービスプロバイダとしてのメーカー側機器（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。なお、ここでは、家電機器（ＥＥ）のセキュリティチップ（ＳＣ）を発行対象としたサービス属性証明書の利用例を示してあるが、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＳＣ）を発行対象としたサービス属性証明書を利用した処理も同様に可能である。ただし、ダイレクトにＳＰとの通信を実行できないユーザ識別デバイス（ＵＩＤ）の場合は、

（１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略

が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ３４３では、セキュリティチップからエンドエンティテイに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ３４４において、セキュリティチップ（ＳＣ）は、メーカー側機器であるサービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対して自己のメモリに格納したサービス属性証明書を送信する。

ユーザ側家電機器のセキュリティチップ（ＳＣ）からサービス属性証明書を受信したメーカー側機器（ＳＰ）のセキュリティモジュール（ＳＭ）は、ステップＳ３４５において、サービス属性証明書の検証処理を実行する。サービス属性証明書の検証処理については、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

サービス属性証明書の検証処理後、セキュリティモジュール（ＳＭ）は、検証結果をメーカー側機器（ＳＰ）に出力し、検証不成立の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、サービス属性証明書の検証が不成立であった旨をエンドエンティテイ通知する処理を実行してもよい。

サービス属性証明書の検証が成功し、サービス属性証明書の正当性が確認されるとステップＳ３４７に進む。ステップＳ３４７では、サービス属性証明書の審査を実行する。審査は、サービスプロバイダとしてのメーカー側機器（ＳＰ）の保有するグループ情報データベースに基づいて実行する。

サービス属性証明書の審査処理について、図４９を参照して説明する。ステップＳ３５１において、サービスプロバイダ（ＳＰ）は、検証済みのサービス属性証明書から属性値としてのグループＩＤを取得する。ステップＳ３５２に

おいて、サービス属性証明書から取得したグループＩＤに基づいて、グループ情報データベースを検索（Ｓ３５２）し、登録されたエントリーから、コントロール属性証明書情報、例えばコントロール属性証明書の識別子（ＩＤ）を取得（Ｓ３５３）する。

図４９に示すように、サービスプロバイダの保有するグループ情報データベース（ＤＢ）には、発行者、サービスＡＣのグループＩＤ、およびグループ情報としての対応コントロール属性証明書情報、例えばＩＤが対応付けられて格納され、サービスプロバイダ（ＳＰ）は、ユーザ側家電機器から受領し、検証の成立したサービス属性証明書（ＡＣ）から取得したグループＩＤに基づいて、グループ情報データベース（ＤＢ）を検索してグループ情報として、サービスＡＣに対応するコントロール属性証明書（ＡＣ）の特定情報を取得する。

次に、サービスプロバイダとしてのメーカー側機器（ＳＰ）は、ステップＳ３４８（図４８）において、グループ情報データベース（ＤＢ）から取得したコントロール属性証明書（ＡＣ）のＩＤに基づいて、コントロール属性証明書（ＡＣ）を取得する。

次に、サービス属性証明書を受領したサービスプロバイダが、コントロール属性証明書に基づくサービス、例えば家電機器に対するメンテナンス、点検、修理、アップグレード、あるいはコントロール等の処理を実行するシーケンスについて、図５０以下を参照して説明する。

図５０のステップＳ３７０において、メーカー側機器を操作するオペレータがメーカー側機器（ＳＰ）の入力インタフェースを介して、コントロール属性証明書を適用したメンテナンス処理実行コマンドを入力する。この処理の際、オペレータは利用するコントロール属性証明書に設定されたグループＩＤを指定する。

メーカー側機器（ＳＰ）がコントロール属性証明書を適用したメンテナンス処理実行要求入力を受領すると、ステップＳ３７１において、家電機器（ＥＥ）のセキュリティチップ（ＳＣ）と、サービスプロバイダとしてのメーカー側機器（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。なお、先に図４８を参照して説明したサービス属性証明書の検証処理シーケンス

と同一セッションで図５０に示すコントロール属性証明書に基づくサービス提供シーケンスが実行される場合は、この相互認証処理は不要となる。

認証処理が実行された場合は、ステップＳ３７２で、セキュリティモジュール（ＳＭ）からメーカー側機器（ＳＰ）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ３７３において、メーカー側機器（ＳＰ）のセキュリティモジュール（ＳＭ）は、ユーザ側家電機器側のセキュリティチップ（ＳＣ）に対して、受信したサービス属性証明書に基づいて抽出したコントロール属性証明書を送信する。このコントロール属性証明書は、先に説明したように、家電機器に対するコントロール範囲処理権限を確認する処理に適用するグループ属性証明書である。

メーカー側機器（ＳＰ）のセキュリティモジュール（ＳＭ）からコントロール属性証明書を受信したセキュリティチップ（ＳＣ）は、ステップＳ３７４において、コントロール属性証明書検証処理を実行する。コントロール属性証明書の検証処理は、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

コントロール属性証明書の検証処理後、セキュリティチップ（ＳＣ）は、検証結果をユーザ側家電機器（ＥＥ）に出力（Ｓ３７５）し、検証不成立の場合（Ｓ３７６：ＮＧ）は、エラー処理（Ｓ３７７）として、メンテナンス等の処理の実行を中止する。この場合、コントロール属性証明書の検証が不成立であった旨をメーカー側機器（ＳＰ）に通知する処理を実行してもよい。

コントロール属性証明書の検証が成功（Ｓ３７６：ＯＫ）し、コントロール属性証明書の正当性が確認されるとステップＳ３７８に進む。ステップＳ３７８では、家電機器（ＥＥ）がメンテナンス実行プログラムの検索を行なう。このメンテナンス実行プログラムは、あらかじめ家電機器（ＥＥ）にコントロール属性証明書ＩＤ、あるいはグループＩＤに対応付けられてメモリに格納されているか、あるいは処理実行時にメーカー側機器（ＳＰ）から送信されるプログラムであり、必要に応じて暗号化されている。このシーケンス図においては、

メンテナンス実行プログラムは、あらかじめ家電機器（ＥＥ）にコントロール属性証明書ＩＤ、あるいはグループＩＤに対応付けられて格納されている場合の例である。

ステップＳ３７９では、家電機器（ＥＥ）が抽出した暗号化メンテナンスプログラムをセキュリティチップ(ＳＣ)に転送し、ステップＳ３８０において、セキュリティチップ（ＳＣ）側において復号処理を実行する。復号処理は、例えばサービスプロバイダ（ＳＰ）側から提供された鍵、あるいは各ユーザデバイスに固有の鍵等に基づいて実行される。プログラムの暗号化処理態様としては、公開鍵方式、共通鍵方式等、各種の処理方式が採用可能である。なお、鍵を格納した属性証明書を利用して鍵をセキュリティチップに提供する構成としてもよい。

ステップＳ３８１において、セキュリティチップ（ＳＣ）から復号されたメンテナンスプログラムが家電機器としてのエンドエンティテイ（ＥＥ）に出力され、ステップＳ３８２において、メンテナンスプログラムが実行され、プログラム実行完了の後、ステップＳ３８３において、実行結果がサービスプロバイダ（ＳＰ）に送信される。

図５１は、図５０と同様、サービス属性証明書を受領したサービスプロバイダが、コントロール属性証明書に基づくサービス、例えば家電機器に対するメンテナンス、点検、修理、アップグレード、あるいはコントロール等の処理を実行するシーケンスであり、メンテナンス実行プログラムをメーカー側機器（ＳＰ)からユーザ側家電機器(ＥＥ)に対して送信する処理とした例である。ステップＳ３８４～Ｓ３９２は、図５０のステップＳ３７０～Ｓ３７７に対応する。

コントロールＡＣの検証ＯＫの後のステップＳ３９３において、ユーザ側家電機器（ＥＥ）からメーカー側機器（ＳＰ）に対してメンテナンスプログラムの送信要求が出力され、ステップＳ３９４において、サービスプロバイダとしてのメーカー側機器がメンテナンスプログラムの検索を実行し、ステップＳ３９５において検索したプログラムをユーザ側家電機器（ＥＥ）に対して送信する処理部分が、図５０の処理シーケンスと異なっている。

なお、送信プログラムは、必要に応じて暗号化される。例えばセッション鍵、サービスプロバイダ（ＳＰ）側から提供された鍵、あるいは各ユーザデバイスに固有の鍵等に基づいて復号可能な態様で暗号化がなされて送信される。プログラムの暗号化処理態様としては、公開鍵方式、共通鍵方式等、各種の処理方式が採用可能である。なお、鍵を格納した属性証明書を利用して鍵をセキュリティチップに提供する構成としてもよい。

図５２の処理シーケンスは、図５０、図５１と同様、サービス属性証明書を受領したサービスプロバイダが、コントロール属性証明書に基づくサービス、例えば家電機器に対するメンテナンス、点検、修理、アップグレード、あるいはコントロール等の処理を実行するシーケンスであるが、メンテナンス実行プログラムをメーカー側機器（ＳＰ）から、逐次コマンドを家電機器（ＥＥ）に送信し、コマンド実行に基づく応答を家電機器（ＥＥ）から受信しながらレスポンス対応の処理を実行する構成としたものである。

ステップＳ４１０～Ｓ４２０は、図５１のステップＳ３８４～Ｓ３９４に対応する。サービスプロバイダ（ＳＰ）は、ステップＳ４２１でメンテナンスプログラムに従ったコマンドを必要に応じて暗号化して家電機器（ＥＥ）に送信し、家電機器（ＥＥ）はステップＳ４２２において、暗号化コマンドをセキュリティチップに渡し、セキュリティチップ（ＳＣ）における復号（Ｓ４２３）、セキュリティチップ（ＳＣ）から復号コマンドの引き渡し（Ｓ４２４）の後、家電機器（ＥＥ）においてコマンドを実行（Ｓ４２５）し、実行結果をコマンド実行レスポンスとして家電機器（ＥＥ）からサービスプロバイダ（ＳＰ）に送信し、レスポンスを受信したサービスプロバイダ（ＳＰ）がレスポンスに基づく次実行コマンドを家電機器（ＥＥ）に送信する構成としている。

メンテナンスプログラムに従ったコマンドの実行がすべて終了すると、ステップＳ４２７において、メンテナンスプログラム実行処理を終了する。

上述したメンテナンス処理形態は、ユーザ側の家電機器からサービス属性証明書を、メーカー側機器に提示し、一方、メーカー側機器がコントロール属性証明書を家電機器に提示して、相互に各属性証明書の検証、審査を実行して、サービスの受領あるいは提供範囲の権限確認を行なう形態である。

サービス属性証明書、コントロール属性証明書の利用形態は上述した処理形態に限らず、例えば図５３に示すように、両属性証明書をユーザー側機器４９１に格納して、サービス提供要求時にサービス属性証明書４９３、コントロール属性証明書４９４をメーカー側（ＳＰ）４９２に提示し、メーカー側（ＳＰ）４９２において、サービス属性証明書４９３、コントロール属性証明書４９４の検証、審査を実行するとともに、両者の対応関係を確認の後、コントロール属性証明書４９４によって示される権限の範囲でのメンテナンス処理をユーザー側機器４９１に対して実行する形態としてもよい。

また、家電機器において一定時間毎にメンテナンス自動実行を行なうプログラムを格納し、プログラムされた時間間隔でサービス属性証明書を伴うメンテナンス要求をメーカー側に送信し、メーカー側が要求受信に基づいて、コントロール属性証明書の送信およびメンテナンス処理を実行する形態としてもよい。

（５－４）パーソナルコミュニュケーションサービス

次に、グループ属性証明書に基づいて権限確認を実行してエンドエンティティ（ＥＥ）としてのＰＣ、ＰＤＡ、その他の通信端末を利用したコミュニケーションサービス利用例について説明する。

ここでは、ＰＣ、ＰＤＡ、その他の通信端末をエンドエンティティ（ＥＥ）として、自宅等に設置した通信端末が、チャットルームを提供するサービスプロバイダのサーバに接続して、チャットルームを介した通信端末間のコミュニケーション、およびエンドエンティティ（ＥＥ）間の直接通信において、グループ属性証明書を利用したアクセス制限処理を実行してコミュニケーションサービスを行なう例を説明する。コミュニケーションサービスにおいて適用するグループ属性証明書の例を図５４に示す。

グループ属性証明書ＡＣ０１は、発行者が、サービスプロバイダ（ＳＰ）としてのチャット運営者であり、所有者、すなわちグループ属性証明書ＡＣ０１の発行時に発行者であるチャット運営サービスプロバイダ（ＳＰ）と認証処理を行なうことによりグループ属性証明書ＡＣ０１の発行対象となった所有者

は、ユーザ甲さんの通信端末としてのエンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ)、あるいはユーザ甲さんのユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）である。

このグループ属性証明書ＡＣ０１は、チャット運営サービスプロバイダ（ＳＰ)の提供するチャットルームを構成するサーバに対するアクセス権を有することを証明する属性証明書であり、チャットルームに対して参加する権限を有するユーザーグループあるいはユーザ機器グループに対して発行される。

グループ属性証明書ＡＣ０２は、発行者が、乙さんのユーザデバイス、（ＥＥまたはＵＩＤ）であり、所有者、すなわちグループ属性証明書ＡＣ０２の発行時に発行者である乙さんのユーザデバイスのセキュリティチップ(ＳＣまたはＵＳＣ)と認証処理を行なうことによりグループ属性証明書ＡＣ０２の発行対象となった所有者は、甲さんのユーザデバイスのセキュリティチップ（ＳＣまたはＵＳＣ）である。

このグループ属性証明書ＡＣ０２は、乙さんのユーザデバイスの管理サーバーへのアクセス権を有することを証明する属性証明書であり、乙さんのユーザデバイスの管理サーバーにアクセスする権限を有するユーザーグループあるいはユーザ機器グループに対して発行される。

なお、グループ属性証明書ＡＣ０１，ＡＣ０２の発行処理は、サービスプロバイダ(ＳＰ)あるいは乙さんユーザデバイスとしてのエンドエンティテイ(ＥＥ）あるいはユーザ識別デバイス（ＵＩＤ）自体が、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）の機能を実行して、みずから発行することが可能であるが、グループ属性認証局（グループＡＡ）およびグループ属性証明書登録局（グループＡＲＡ）に依頼して発行処理を行なう構成も可能である。ただし、この場合には発行者のポリシーに従った処理が実行されることが条件である。

例えばグループ属性証明書ＡＣ０１、ＡＣ０２の発行処理は、発行者であるサービスプロバイダ（ＳＰ)、乙さんのユーザデバイス（ＥＥ，ＵＩＤ)、あるいは、発行代理を行なうグループ属性証明書登録局（グループＡＲＡ）が、発行要求者としての甲さんから、甲さんであることを証明する既発行のグループ

属性証明書、例えばクレジットカード会社の発行したグループ属性証明書を提示させ、その提出されたグループ属性証明書の検証を実行した後、新たなグループ属性証明書ＡＣ０１、ＡＣ０２の発行処理を行なう方法をとることが好ましい。このような既発行のグループ属性証明書の検証を条件として、新たなグループ属性証明書を発行する処理シーケンスは、先に図２９、図３０、図３２等を参照して説明した処理シーケンスと同様となる。

図５４に示すグループ属性証明書の発行、格納形態は、図５５に示す通りとなる。チャットルーム提供サービスプロバイダ（ＳＰ）５０１と、エンドエンティテイとしての甲さん通信端末（ＥＥ）５１１、乙さん通信端末（ＥＥ）５３１は通信ネットワークにより相互にデータ転送可能であり、通信端末（ＥＥ）５１１とユーザ識別デバイス（ＵＩＤ）５２１、通信端末（ＥＥ）５３１とユーザ識別デバイス（ＵＩＤ）５３３は、双方の接続機器インタフェース２３１（図９参照）を介して相互にデータ転送が可能である。

それぞれの機器には、耐タンパ構成を持つ（ユーザ）セキュリティチップ５１２，５２２，５３２，５３４またはセキュリティモジュール５０２が備えられ、データ通信処理の際の相互認証処理、あるいは転送データの暗号化、復号処理等を実行する。またグループ属性証明書の検証処理もこれらセキュリティチップ、セキュリティモジュールにおいて実行される。

甲さんのユーザ識別デバイス５２１には、先に図５４を参照して説明したグループ属性証明書ＡＣ０１，５２３が格納される。グループ属性証明書ＡＣ０１，５２３は、発行者が、チャットルーム提供サービスプロバイダ（ＳＰ）５０１であり、チャットルーム参加権限確認処理に適用され、所有者である甲さんユーザデバイスのＵＳＣ５２１からチャットルーム提供サービスプロバイダ（ＳＰ）５０１に送付されて、チャットルーム提供サービスプロバイダ（ＳＰ）５０１のセキュリティモジュール（ＳＭ）５０２において、グループ属性証明書ＡＣ０１の検証、審査の後、サービス、すなわちチャットルーム参加が認められる。

また、甲さんのユーザ識別デバイス５２１には、先に図５４を参照して説明したグループ属性証明書ＡＣ０２，５２４も格納される。グループ属性証明書

ＡＣ０２，５２４は、発行者が、乙さんユーザデバイス（ＥＥ５３１またはＵＩＤ５３３）であり、乙さんのユーザデバイスの管理サーバーに対するアクセス権限確認処理に適用され、所有者である甲さんユーザデバイスのＵＳＣ５２１から乙さんユーザデバイス（ＥＥ５３１またはＵＩＤ５３３）に送付されて、乙さんユーザデバイス（ＥＥ５３１またはＵＩＤ５３３）のセキュリティチップ（ＳＣ５３２またはＵＳＣ５３４）において、グループ属性証明書ＡＣ０２の検証、審査の後、サービス、すなわち乙さんデバイスの管理サーバーに対するアクセスが認められる。

図５６を参照して、甲さんのユーザ識別デバイス４２１に格納されたグループ属性証明書ＡＣ０１，５２３を適用してチャットルーム参加サービスの利用権限確認処理を行ない、サービスを開始する処理シーケンスについて説明する。図５６において、

ＵＩＤ：甲さんユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：ＵＩＤ内に構成されるユーザセキュリティチップ、

ＥＥ：甲さん通信端末（ＥＥ）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

ＳＰ：チャットルーム提供サービスプロバイダ（ＳＰ）制御部、

ＳＭ：ＳＰ内のセキュリティモジュール、

である。

まず、ステップＳ４５１において、ユーザ（甲さん）がエンドエンティティとしての甲さん通信端末（ＥＥ）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）＝ＡＣ０１の利用要求コマンドを入力する。このグループ属性証明書（Ｇｐ．ＡＣ）は、図５４、図５５に示すＡＣ０１である。この処理の際、ユーザは利用するグループ属性証明書ＡＣ０１に設定されたグループＩＤを指定する。ただし、特定のサービスを指定することにより唯一のグループＩＤが決定可能である場合は、サービスの指定のみとしてもよい。

甲さん通信端末（ＥＥ）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１の利用要求入力を受領すると、ステップＳ４５２において、ユーザセキュリティチップ（ＵＳＣ）と、サービスプロバイダとしてのチャットルーム

提供サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証が実行される。なお、ここでは省略して示してあるが、ダイレクトにＳＰとの通信を実行できないユーザ識別デバイス（ＵＩＤ）の場合は、

（１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ４５３では、ユーザセキュリティチップからエンドエンティテイに対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ４５４において、ユーザセキュリティチップ（ＵＳＣ）は、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）に対して自己のメモリに格納したグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）は、先に図５４、図５５を参照して説明したように、チャットルームへの参加資格権限を判定する処理に適用するグループ属性証明書ＡＣ０１である。

ユーザセキュリティチップ（ＵＳＣ）からグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１を受信したチャットルーム提供サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）は、ステップＳ４５５において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

グループ属性証明書（Ｇｐ．ＡＣ）の検証処理後、セキュリティモジュール（ＳＭ）は、検証結果をチャットルーム提供サービスプロバイダ（ＳＰ）に出力し、検証不成立の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨をエンドエンティテイに通知する処理を実行してもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ４５７に進む。ステップＳ４５７では、先に図２５を参照して説明したグループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、サービスプロバイダとしてのチャットルーム提供サービスプロバイダ（ＳＰ）の保有するグループ情報データベースに基づいて実行する。すなわち、チャットルーム提供サービスプロバイダ（ＳＰ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０１から発行者情報、グループＩＤを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

この場合のグループ情報は、チャットルームへの参加許可情報を含むものである。サービスプロバイダとしてのチャットルーム提供サービスプロバイダ（ＳＰ）は、ステップＳ４５８において、サービス提供処理、すなわち、グループ情報に従って、チャットルームへの参加許可を行なう。すなわち、チャットルームを提供するサーバーへのアクセスを許可する処理を行なう。

次に、図５７を参照して、甲さんのユーザ識別デバイス４２１に格納されたグループ属性証明書ＡＣ０２，５２４を適用して乙さんのユーザデバイスへのアクセス権限確認処理を行ない、甲さんおよび乙さんとのコミュニケーションを開始する処理シーケンスについて説明する。図５７において、

ＵＩＤ：甲さんユーザ識別デバイス（ユーザデバイス）制御部、

ＵＳＣ：ＵＩＤ内に構成されるユーザセキュリティチップ、

ＥＥ１：甲さん通信端末（ＥＥ）制御部、

ＳＣ１：ＥＥ１内に構成されるセキュリティチップ、

ＥＥ２：乙さん通信端末（ＥＥ）制御部、

ＳＣ２：ＥＥ２内に構成されるセキュリティチップ、

である。

まず、ステップＳ４６１において、ユーザ（甲さん）がエンドエンティテイとしての甲さん通信端末（ＥＥ１）の入力インタフェースを介して、グループ属性証明書（Ｇｐ．ＡＣ）＝ＡＣ０２の利用要求コマンドを入力する。このグループ属性証明書（Ｇｐ．ＡＣ）は、図５４、図５５に示すＡＣ０２である。この処理の際、ユーザは利用するグループ属性証明書ＡＣ０２に設定されたグループＩＤを指定する。

甲さん通信端末（ＥＥ１）がユーザからのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２の利用要求入力を受領すると、ステップＳ４６２において、ユーザセキュリティチップ（ＵＳＣ）と、乙さんユーザデバイスのセキュリティチップ（ＳＣ２）間の相互認証が実行される。なお、ここでは、グループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２は、乙さん通信端末（ＥＥ）のセキュリティチップ（ＳＣ２）が発行主体であった例を説明する。発行主体が乙さんのユーザ識別デバイス（ＵＩＤ）である場合は、乙さんのユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）との認証を行なうことになる。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。ステップＳ４６３では、甲さんのユーザセキュリティチップ（ＵＳＣ）からエンドエンティテイ（ＥＥ１）に対して、相互認証の成立、不成立の結果情報を含む相互認証完了通知が出力される。相互認証不成立の場合は、処理の続行は中止される。相互認証が成立すると、ステップＳ４６４において、ユーザセキュリティチップ（ＵＳＣ）は、乙さん通信端末（ＥＥ）のセキュリティチップ（ＳＣ２）に対して自己のメモリに格納したグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２を送信する。このグループ属性証明書（Ｇｐ．ＡＣ）は、先に図５４、図５５を参照して説明したように、乙さんのユーザデバイスのサーバーへのアクセス権限を判定する処理に適用するグループ属性証明書ＡＣ０２である。

ユーザセキュリティチップ（ＵＳＣ）からグループ属性証明書（Ｇｐ．ＡＣ）

ＡＣ０２を受信した乙さん通信端末（ＥＥ）のセキュリティチップ（ＳＣ２）は、ステップＳ４６５において、グループ属性証明書検証処理を実行する。グループ属性証明書の検証処理については、先に図２１乃至図２３を参照して説明した通りであり、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

グループ属性証明書（Ｇｐ．ＡＣ）の検証処理後、乙さん通信端末（ＥＥ）のセキュリティチップ（ＳＣ２）は、検証結果を乙さん通信端末（ＥＥ）に出力し、検証不成立の場合は、エラー処理として、サービス提供を実行せず処理を中止する。この場合、グループＡＣの検証が不成立であった旨を甲さん側に通知する処理を実行してもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ４６７に進む。ステップＳ４６７では、先に図２５を参照して説明したグループ属性証明書（Ｇｐ．ＡＣ）の審査を実行する。審査は、乙さん通信端末（ＥＥ）の保有するグループ情報データベースに基づいて実行する。すなわち、乙さん通信端末（ＥＥ）は、検証済みのグループ属性証明書（Ｇｐ．ＡＣ）ＡＣ０２から発行者情報、グループＩＤを取得し、取得情報に基づいて、グループ情報データベースを検索し、登録されたエントリーの有無を確認する。対応する登録エントリーがある場合は、グループ情報データベースからグループ情報を取得する。

この場合のグループ情報は、乙さんユーザデバイスのサーバーへのアクセス権限情報を含むものである。乙さん通信端末（ＥＥ）は、ステップＳ４６８において、サービス提供処理、すなわち、グループ情報に従って、乙さんユーザデバイスのサーバーへのアクセス許可を行なう。

［（６）実行属性証明書（実行ＡＣ）］

次に、属性証明書を利用した権限確認に基づくサービス提供処理態様において、属性証明書に基づいてサービス受領権限を判定するのみならず、サービスの実行自体を属性証明書によって制限することを可能とした実行属性証明書（実行ＡＣ）について説明する。

（６－１）実行属性証明書概要

上述したグループ属性証明書、あるいは従来から知られる一般的な属性証明書は、所有者の属性としての権限情報等、属性証明書の格納データが改竄されていないことを署名検証により検証することができる。以下、説明する実行属性証明書（実行ＡＣ）は、検証により、証明書が改竄されていないことの確認を実行するのみならず、さらに、証明書所有者が実行属性証明書に格納した暗号化データ（プログラム）を復号して、暗号化データ（プログラム）の復号に基づいてサービスを受領する構成を持つ。

実行属性証明書に格納した暗号化データ（プログラム）を復号するために適用する鍵（登録鍵）は、実行属性証明書発行者と、実行属性証明書の所有者としてのサービス受領者に対応するユーザデバイスのセキュリティチップ（ＳＣ）のみが知り得る秘密の共通鍵である。従って、特定のユーザデバイスにおいてのみ実行属性証明書に基づくサービス実行が可能となる。

なお、以下の説明においては、ユーザデバイスであるエンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）が実行属性証明書の処理を行なうものとして説明するが、以下に説明するセキュリティチップ（ＳＣ）での処理は、前述したグループ属性証明書における処理と同様、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）においても同様に実行可能な処理である。

実行属性証明書は、図５８（ａ）に示すように、提供サービスの実行に必要となるプログラム等の実行命令を登録鍵で暗号化したデータと、登録鍵を格納したセキュリティチップのメモリ、例えば図５８（ｃ）に示すセキュリティチップのＥＥＰＲＯＭ２０６内に形成される共通鍵メモリ領域２０７における登録鍵格納領域を示すアドレスデータとしてのメモリ領域ブロックアドレスを有する。その他、各種の属性証明書データ（図５参照）を有し、発行者署名を付したものである。データの改竄検証は、署名検証により実行可能である。署名生成、検証処理は、先に図１７、図１８を参照して説明した処理に従って実行可能である。

なお、実行属性証明書は、属性証明書の基本フォーマット、例えば ITU-T X.509 に準拠したものとして構成可能である。ただし、ITU-T X.509 で規定されたフォーマットに従うことが必須ではなく、独自フォーマットとした実行属性証明書を構成してもよい。

セキュリティチップ（ＳＣ）の共通鍵メモリ領域２０７には、図５８（ｂ）に示すように、ユーザデバイスとしてのエンドエンティテイ（ＥＥ）の有する複数の実行属性証明書に対応する複数の登録鍵が所定のブロックアドレスに対して格納される。

共通鍵メモリ領域２０７は、例えば６４ビットなどある固定されたサイズのブロックから構成される不揮発性メモリのメモリ領域である。登録鍵の格納処理、およびリセット処理は、所定の手続きに従って実行される。この処理については後述する。リセット命令を除き、登録鍵格納メモリ領域へのアクセスは、アクセスするブロックに格納された登録鍵で暗号化された命令を用いることによってのみ実行可能となる。また、秘密鍵についても、秘密鍵を読み出せない仕組みに加え、入力したデータを秘密鍵で暗号化または復号化した結果を直接読み出すことは出来ないような、仕組みを持っているものとする。ここで、直接読み出すことが出来ないというのは、例えば、ハッシュをかけた後、秘密鍵で暗号化することや、公開鍵で暗号化した命令を、秘密鍵で復号して実行することはできることを意味する。以下、実行属性証明書の所有者であるセキュリティチップあるいはモジュールは、この仕組みを持つものとする。

実行属性証明書の利用手続き概要を図５９に示すフローに従って説明する。図５９は、例えば実行属性証明書の発行者としてのサービスプロバイダ（ＳＰ）と、実行属性証明書によるサービス受領者としてのユーザデバイスにおける処理の該略を示すフローである。ステップＳ５０１において、サービスプロバイダ（ＳＰ）とユーザデバイス間で相互認証が実行され、ステップＳ５０２において、例えば前述したグループ属性証明書に基づくサービス利用権限の審査が実行される。ここでの処理は、前述したグループ属性証明書における認証処理、検証処理と同様であり、認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を

参照して説明した公開鍵方式の相互認証処理として実行される。検証処理は、先に図２１乃至図２３を参照して説明した、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

次にステップＳ５０３の処理として、実行属性証明書（実行ＡＣ）に基づくサービス提供処理が行なわれる。実行属性証明書（実行ＡＣ）に基づくサービス提供処理は、ステップＳ５０４に示す実行属性証明書（実行ＡＣ）の発行処理、ステップＳ５０５に示す実行属性証明書（実行ＡＣ）の適用処理、ステップＳ５０６に示す実行属性証明書（実行ＡＣ）の破棄処理のいずれかの態様で実行されることになる。以下、これらの処理の詳細について、図を参照して説明する。

（６－２）実行属性証明書発行処理

まず、実行属性証明書発行処理について説明する。図６０に実行属性証明書の発行シーケンス図を示す。図６０において、

ＥＥ：ユーザデバイスのエンドエンティテイ（ＥＥ）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

実行ＡＣテーブル:実行ＡＣの管理テーブル格納メモリおよびメモリ制御部

ＳＰ：実行ＡＣの発行処理を実行するサービスプロバイダ機器（ＳＰ）制御部、

ＳＭ：ＳＰ内のセキュリティモジュール、

である。

まず、ステップＳ５１１において、ユーザがユーザデバイスとしてのエンドエンティテイ（ＥＥ）の入力インタフェースを介して、実行属性証明書（実行ＡＣ）発行要求コマンドを入力する。エンドエンティテイ（ＥＥ）がユーザからの実行属性証明書の発行要求を受領すると、ステップＳ５１２において、セキュリティチップ（ＳＣ）と、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証、および実行属性証明書（実行ＡＣ）発行条件として適用される発行済みのグループ属性証明書の検証、審査処理が行なわれ

る。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。検証処理は、先に図２１乃至図２３を参照して説明した、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

なお、ここでは、エンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）を発行対象とした実行属性証明書の発行処理例を示してあるが、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）を発行対象とした実行属性証明書発行処理の場合は、

（１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

ステップＳ５１２の認証、グループ属性証明書の検証、審査がすべて成立すると、サービスプロバイダ（ＳＰ）は、ユーザデバイスのエンドエンティテイ（ＥＥ）に対して、登録鍵生成実行ＡＣ生成情報要求処理を行なう。これは、具体的には、実行属性証明書の実行命令（図５８参照）の暗号化、復号化処理に適用する登録鍵の格納領域として使用するメモリのメモリ領域空きアドレスを要求する処理である。

エンドエンティテイ（ＥＥ）は、登録鍵生成実行ＡＣ生成情報要求を受信すると、ステップＳ５１４において、登録鍵の格納領域として使用するメモリのメモリ領域空きアドレス検索を実行ＡＣテーブル制御部に対して出力し、実行ＡＣテーブル（制御部）がこの要求に応じて、実行ＡＣテーブルを参照して、新規登録用の登録鍵を格納すべきメモリ領域空きアドレスをエンドエンティ

テイに通知する。実行ＡＣテーブルは、例えば図６２に示すように、サービスプロバイダの識別データとしてのＳＰ情報、サービスプロバイダの提供するサービス情報、例えば暗号化コンテンツ情報、サービスプロバイダの提供するサービス情報利用のために必要となるプログラムを実行命令として格納した実行ＡＣとを対応付けたテーブルである。実行ＡＣテーブルは、エンドエンティテイ（ＥＥ）またはセキュリティチップ（ＳＣ）内のメモリに格納される。

実行ＡＣテーブル（制御部）は、すでに格納済みの実行ＡＣに対応する登録鍵のメモリ領域ブロックアドレスを参照して、自己のセキュリティチップにおける空きアドレスを検出して、新規登録用の登録鍵を格納すべきメモリ領域空きアドレスをエンドエンティテイに通知する。実行ＡＣテーブル制御部は、実行ＡＣテーブルを格納したメモリのアクセス制御、データ抽出を実行し、エンドエンティテイ（ＥＥ）またはセキュリティチップ（ＳＣ）のメモリアクセス制御処理を実行するＣＰＵ等により構成される制御部である。

エンドエンティテイ（ＥＥ）は、ステップＳ５１６において、空きアドレスをサービスプロバイダ（ＳＰ）に送信する。新規登録鍵のメモリ領域ブロックアドレスを受信したサービスプロバイダ（ＳＰ）は、ステップＳ５１７において、登録鍵生成実行ＡＣの生成要求をセキュリティモジュール（ＳＭ）に出力し、ステップＳ５１８において、セキュリティモジュール（ＳＭ）は、登録鍵生成実行ＡＣの生成処理を行なう。サービスプロバイダ（ＳＰ）からセキュリティモジュール（ＳＭ）に対して出力される登録鍵生成実行ＡＣの生成要求には、セキュリティチップ公開鍵（ＫｐＳＣ）を格納したセキュリティチップ公開鍵証明書、登録鍵のリセット時に適用するリセット鍵（Ｋｒｅｓｅｔ）、登録鍵生成命令（ＧｅｎＫｅｒ）、メモリ領域ブロックアドレス（Ａｄ）が含まれる。

図６３を参照して、セキュリティモジュール（ＳＭ）における登録鍵生成実行ＡＣの生成処理の詳細を説明する。

セキュリティモジュール（ＳＭ）６０１は、先に図９を参照して説明したセキュリティチップ構成と同様の構成であり、図６３は、その構成中の暗号処理部、メモリ部を抽出して示すものである。暗号処理部としては、公開鍵暗号エ

ンジン６０２、共通鍵暗号エンジン６０３を有する。セキュリティモジュール（ＳＭ）６０１は、先に、図９を参照して説明したように、ＣＰＵ，ＲＡＭ，ＲＯＭ等の構成を持ち、その他のデータ処理、データ入出力処理が可能である。

公開鍵暗号エンジン６０２は、楕円曲線暗号、あるいはＲＳＡ（Rivest-Shamir-Adleman）暗号処理等の公開鍵方式の暗号処理を実行し、データの暗号化、復号化、署名生成、検証処理等を行なう。共通鍵暗号エンジン６０３は、例えばＤＥＳ、トリプルＤＥＳ等の共通鍵暗号方式の暗号処理を実行し、データの暗号化、復号化等を行なう。なお、セキュリティモジュール（ＳＭ）６０１は、さらにハッシュ生成処理、乱数発生処理機能を持つ。

セキュリティモジュール（ＳＭ）は、上述したように登録鍵生成実行ＡＣ生成要求に伴い、セキュリティチップ公開鍵（ＫｐＳＣ）を格納したセキュリティチップ公開鍵証明書、登録鍵のリセット時に適用するリセット鍵（Ｋｒｅｓｅｔ）、登録鍵生成命令（ＧｅｎＫｅｒ）、メモリ領域ブロックアドレス（Ａｄ）を入力する。

ステップＳ５４１の乱数発生処理において、発生した乱数に基づくセッション鍵（Ｋｃｓ）と登録鍵生成命令（ＧｅｎＫｅｒ）がステップＳ５４２において、セキュリティチップ公開鍵（ＫｐＳＣ）を用いて暗号化され、暗号化データ（Ｅｐ（ＧｅｎＫｃｒ||Ｋｃｓ；ＫｐＳＣ）が生成される。なお、ａ||ｂはａ，ｂの連結データを示し、Ｅｐ（ａ；ｂ）は、鍵ｂを適用したａの公開鍵暗号方式に基づく暗号化メッセージを示す。

次に、ステップＳ５４３において、実行命令付加処理が行なわれる。Ｄｐｃ［ａ］は、公開鍵暗号方式に基づく秘密鍵による復号に基づいてデータａ内のコマンドを実行する実行命令を示す。さらに、ステップＳ５４４において、リセット鍵（Ｋｒｅｓｅｔ）に基づく共通鍵方式の暗号化処理が実行され、暗号化データ（Ｅｃ（Ｄｐｃ［Ｅｐ（ＧｅｎＫｃｒ||Ｋｃｓ；ＫｐＳＣ)］；Ｋｒｅｓｅｔ）が生成される。なお、Ｅｃ（ａ；ｂ）は、鍵ｂを適用したａの共通鍵暗号方式に基づく暗号化メッセージを示す。

さらに、ステップＳ５４５において、上記暗号化データ（Ｅｃ（Ｄｐｃ［Ｅｐ（ＧｅｎＫｃｒ||Ｋｃｓ；ＫｐＳＣ)］；Ｋｒｅｓｅｔ）と、新規登録鍵の

格納領域を示すメモリ領域ブロックアドレス(Ａｄ)との連結データに対して、セキュリティモジュール（ＳＭ）の秘密鍵（ＫｓＳＭ）を適用した署名処理が実行される。これらの処理の結果、登録鍵生成実行ＡＣ６１１が生成される。

登録鍵生成実行ＡＣ６１１は、

新規登録鍵の格納領域を示すメモリ領域ブロックアドレス（Ａｄ）、

暗号化データ（Ｅｃ（Ｄｐｃ［Ｅｐ（ＧｅｎＫｃｒ||Ｋｃｓ；ＫｐＳＣ)]；Ｋｒｅｓｅｔ))、および、

署名データ、Ｅｐ（Ｈ（Ａｄ||Ｅｃ（Ｄｐｃ［Ｅｐ（ＧｅｎＫｃｒ||Ｋｃｓ；ＫｐＳＣ)]；Ｋｒｅｓｅｔ；ＫｓＳＭ）を含む構成となる。なお、Ｈ（ａ）は、ａのハッシュ値を示す。

図６０のシーケンス図に戻り、説明を続ける。ステップＳ５１８においてセキュリティモジュール（ＳＭ）における登録鍵生成実行ＡＣ生成処理が終了すると、セキュリティモジュール（ＳＭ）からサービスプロバイダ（ＳＰ）に登録鍵生成実行ＡＣが送付され、ステップＳ５１９において、サービスプロバイダ（ＳＰ）から、ユーザデバイスのエンドエンティテイ（ＥＥ）に登録鍵生成実行ＡＣが送付される。

ステップＳ５２０において、ユーザデバイスのエンドエンティテイ（ＥＥ）は、実行ＡＣテーブル（図６２参照）の更新要求を実行ＡＣテーブル（制御部）に送信し、実行ＡＣテーブル（制御部）は、ステップＳ５２１において実行ＡＣテーブル更新を行なう。実行ＡＣテーブル（図６２参照）の更新要求には、新規登録鍵を適用して利用可能なコンテンツ情報、サービスプロバイダ情報、メモリ領域ブロックアドレスが含まれ、実行ＡＣテーブルに対する新規エントリデータとして、これらの情報を登録する。

さらに、ユーザデバイスのエンドエンティテイ（ＥＥ）は、ステップＳ５２２において、セキュリティチップ（ＳＣ）に対して、登録鍵生成要求を出力する。この要求は、登録鍵生成実行ＡＣをセキュリティチップ（ＳＣ）に対して送付する処理として行われる。

セキュリティチップ（ＳＣ）は、ステップＳ５２３において登録鍵生成処理を実行する。セキュリティチップで実行される登録鍵生成実行ＡＣに基づく登

録鍵生成処理について、図６４を参照して説明する。

セキュリティチップ（ＳＣ）６０５は、先に図９を参照して説明したセキュリティチップ構成と同様の構成である。ただし、図５８において説明したように、共通鍵メモリ領域を有する。図６４は、その構成中の暗号処理部、メモリ部を抽出して示すものである。暗号処理部としては、公開鍵暗号エンジン６０６、共通鍵暗号エンジン６０７を有し、メモリ部として共通鍵メモリ領域６０８を有する。セキュリティチップ（ＳＣ）６０５は、先に、図９を参照して説明したように、ＣＰＵ，ＲＡＭ，ＲＯＭ等の構成を持ち、その他のデータ処理、例えば暗号処理部において復号された実行命令に基づくデータ処理、データ入出力処理等も実行可能である。例えば共通鍵メモリ６０８に対するデータの書き込み、読み取り、外部からのデータ入力、外部へのデータ出力、各素子間のデータ転送等のデータ処理はＣＰＵの制御を中心として実行される。

公開鍵暗号エンジン６０６は、楕円曲線暗号、あるいはＲＳＡ（Rivest-Shamir-Adleman）暗号処理等の公開鍵方式の暗号処理を実行し、データの暗号化、復号化、署名生成、検証処理等を行なう。共通鍵暗号エンジン６０７は、例えばＤＥＳ、トリプルＤＥＳ等の共通鍵暗号方式の暗号処理を実行し、データの暗号化、復号化等を行なう。共通鍵メモリ領域６０８は、登録鍵を格納するメモリであり、例えば６４ビットなどある固定されたサイズのブロックから構成される不揮発性メモリからなるメモリである。なお、セキュリティチップ（ＳＣ）６０５は、さらにハッシュ生成処理、乱数発生処理機能を持つ。

セキュリティチップ（ＳＣ）は、上述したようにエンドエンティティからの登録鍵生成要求に伴い、登録鍵生成実行ＡＣ６１１を入力する。

ステップＳ５５１において、リセット鍵（Ｋｒｅｓｅｔ）を適用した共通鍵方式の復号処理によって、登録鍵生成実行ＡＣ６１１の実行命令データ（Ｄｐｃ［Ｅｐ（ＧｅｎＫｃｒ||Ｋｃｓ；ＫｐＳＣ)］が取り出され、さらに、ステップＳ５５２において、復号した実行命令に対応するデータ処理として、セキュリティチップの秘密鍵（ＫｓＳＣ）を適用した公開鍵方式の復号処理によって、登録鍵生成命令（ＧｅｎＫｅｒ）と、セッション鍵（Ｋｃｓ）との連結デ

ータが取り出される。

次のステップＳ５５３も、復号実行命令に対応するデータ処理であり、登録鍵生成命令（ＧｅｎＫｅｒ）の実行処理ステップである。ステップＳ５５４において乱数に基づく登録鍵（Ｋｃｒ）を生成し、ステップＳ５５５において、登録鍵（Ｋｃｒ）を登録鍵の格納領域アドレスであるメモリ領域ブロックアドレス（Ａｄ）に従って、共通鍵メモリ領域６０８に書き込む。

さらに、ステップＳ５５６において、登録鍵（Ｋｃｒ）とメモリ領域ブロックアドレス（Ａｄ）との連結データをセッション鍵（Ｋｃｓ）で暗号化して、登録鍵生成結果６１２として、エンドエンティテイ（ＥＥ）に出力する。

登録鍵生成結果６１２のエンドエンティテイ（ＥＥ）への出力ステップは図６１におけるステップＳ５２４に相当する。

登録鍵（Ｋｃｒ）とメモリ領域ブロックアドレス（Ａｄ）との連結データをセッション鍵（Ｋｃｓ）で暗号化した登録鍵生成結果は、ユーザデバイスのエンドエンティテイ（ＥＥ）から、サービスプロバイダ（ＳＰ）に送信される。

サービスプロバイダ（ＳＰ）は、登録鍵生成結果を受信すると、ステップＳ５２６において、登録鍵生成結果をセキュリティモジュール（ＳＭ）に送付することにより、サービス提供実行ＡＣの生成要求を行なう。セキュリティモジュール（ＳＭ）は、ステップＳ５２７において、サービス提供実行ＡＣの生成処理を実行する。

セキュリティモジュール（ＳＭ）によるサービス提供実行ＡＣの生成処理を図６５を参照して説明する。

まず、ステップＳ５６１において、セッション鍵（Ｋｃｓ）を適用して、登録鍵生成結果の復号処理を実行し、登録鍵（Ｋｃｒ）とメモリ領域ブロックアドレス（Ａｄ）との連結データ（Ａｄ||Ｋｃｒ）を取得する。さらに、ステップＳ５６２において、サービス提供実行ＡＣに格納する実行命令（ＤｅｃＥＤａｔａ||Ｋｃｄ）６１３を登録鍵（Ｋｃｒ）を適用して暗号化する。なお、実行命令は、サービス提供実行ＡＣに応じて設定される実行プログラム等の実行命令である。ここでは、データ復号鍵（Ｋｃｄ）と、暗号化データの復号命令（ＤｅｃＥＤａｔａ）との連結データによって構成された実行命令を例とし

て示している。

さらに、ステップＳ５６３において、実行命令（ＤｅｃＥＤａｔａ||Ｋｃｄ）６１３を登録鍵（Ｋｃｒ）で暗号化したデータ（Ｅｃ（ＤｅｃＥＤａｔａ||Ｋｃｄ）；Ｋｃｒ）と、登録鍵（Ｋｃｒ）を格納するユーザデバイスにおけるセキュリティチップのメモリ領域ブロックアドレス（Ａｄ）とのデータに対して、セキュリティモジュールの秘密鍵（ＫｓＳＭ）によって署名（図１７参照）が生成され、サービス提供実行ＡＣ６１４が生成される。ここでは、サービス提供実行ＡＣ６１４は、暗号化データの復号処理をサービスとして実行する実行属性証明書である。

この実行属性証明書に格納される実行命令を復号するためには、登録鍵（Ｋｃｒ）の適用が必須となり、登録鍵の情報を有するのは、ここでは、このサービス提供実行ＡＣの生成プロセスに参加しているユーザデバイスのセキュリティチップ（ＳＣ）およびサービスプロバイダのセキュリティモジュール（ＳＭ）のみとなる。

図６１に戻りシーケンス図の説明を続ける。ステップＳ５２７において、セキュリティモジュール（ＳＭ）がサービス提供実行ＡＣを生成すると、サービス提供実行ＡＣはステップＳ５２８において、サービスプロバイダ（ＳＰ）からユーザデバイスのエンドエンティテイ（ＥＥ）に送付され、さらに、ステップＳ５２９において、実行ＡＣテーブル制御部に送付されて、ステップＳ５３０において、実行ＡＣテーブル（図６２参照）内に格納される。

上述のプロセスにより、図５８（ａ）に示すように、登録鍵を格納したユーザデバイスのセキュリティチップのメモリ領域ブロックアドレスと、その登録鍵で暗号化された実行命令と、さらに発行者署名、以上の各データを有する実行属性証明書（実行ＡＣ）がユーザデバイスに格納されることになる。なお、これらのデータ以外にも、先に図５を参照して説明したグループ属性証明書の各フィールドのデータを格納することは任意である。ただし、署名は、改竄チェック対象となるデータ全体に対して実行することが必要となる。

（６－３）実行属性証明書適用処理

次に、上述の手続きにおいて発行された実行属性証明書の適用処理について説明する。図６６は、サービス提供実行ＡＣのユーザデバイス側における適用シーケンスをまとめた図である。すでに、前述の処理によって、ユーザデバイスの実行ＡＣテーブルにサービス提供実行ＡＣが格納済みである。

ステップＳ５７１において、ユーザがエンドエンティテイ（ＥＥ）のユーザインタフェースを介してサービス提供実行ＡＣの適用処理要求を入力する。この処理要求には、実行ＡＣの識別子、またはサービスプロバイダ（ＳＰ）情報、サービス内容を特定するデータ、例えば利用コンテンツ、利用プログラムの指定データが含まれる。エンドエンティテイ（ＥＥ）は、ステップＳ５７２において、ユーザ指定のサービス提供実行ＡＣの検索要求を実行ＡＣテーブルに出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ（ＳＰ）情報等である。

ステップＳ５７３において、実行ＡＣテーブルは、エンドエンティテイからの入力キーに基づいて、対応するサービス提供実行ＡＣを検索し、ステップＳ５７４において、テーブルから抽出したサービス提供実行ＡＣをエンドエンティテイ（ＥＥ）に出力する。

ステップＳ５７５において、エンドエンティテイ（ＥＥ）は、受領ＡＣをセキュリティチップ（ＳＣ）に出力し、サービス提供実行ＡＣの適用処理要求を行なう。セキュリティチップは、ステップＳ５７６において、受領ＡＣの提供処理、すなわち、実行属性証明書（実行ＡＣ）に従ったサービス提供を行なう。

セキュリティチップ（ＳＣ）におけるステップＳ５７６のサービス提供処理の詳細を図６７を参照して説明する。セキュリティチップ６０５は、サービス提供実行ＡＣ６１４を入力する。

サービス提供実行ＡＣ６１４は、実行命令（ＤｅｃＥＤａｔａ||Ｋｃｄ）を登録鍵（Ｋｃｒ）で暗号化したデータ（Ｅｃ（ＤｅｃＥＤａｔａ||Ｋｃｄ）；Ｋｃｒ）と、登録鍵（Ｋｃｒ）を格納するユーザデバイスにおけるセキュリティチップのメモリ領域ブロックアドレス（Ａｄ）と、各データに対して、セキュリティモジュールの秘密鍵（ＫｓＳＭ）によって署名したデータを含む。

セキュリティチップ６０５は、ステップＳ５８１において、サービス提供実

行ＡＣ内のメモリ領域ブロックアドレス（Ａｄ）に従って、共通鍵メモリ領域６０８から登録鍵（Ｋｃｒ）を取得し、取得した登録鍵（Ｋｃｒ）によって、サービス提供実行ＡＣ内の暗号化データ（Ｅｃ（ＤｅｃＥＤａｔａ||Ｋｃｄ）；Ｋｃｒ）の復号処理を実行し、データ復号鍵（Ｋｃｄ）と、暗号化データの復号命令（ＤｅｃＥＤａｔａ）を取得する。

ステップＳ５８２において、復号した実行命令に基づくデータ処理が実行される。すなわち、データ復号鍵（Ｋｃｄ）を適用して、外部から入力される復号対象の暗号化データ（Ｅｃ（データ；Ｋｃｄ））６１５の復号処理を実行し、復号されたデータ６１６を出力する。復号対象の暗号化データ（Ｅｃ（データ；Ｋｃｄ））６１５は、例えば画像、音楽、プログラム等のコンテンツを、鍵（Ｋｃｄ）により暗号化したデータであり、サービス提供実行ＡＣ内の格納実行命令を登録鍵（Ｋｃｒ）によって復号することによって取得可能なデータ復号鍵（Ｋｃｄ）によって復号可能となる。

図６６のシーケンス図に戻り説明を続ける。ステップＳ５７６のサービス提供の後、セキュリティチップ（ＳＣ）は、ステップＳ５７７において、登録鍵破棄処理を行なう。この登録鍵破棄処理は、サービス提供実行ＡＣに応じて実行する場合と実行不要となる場合とがある。サービス提供実行ＡＣに基づくサービス提供処理を一度限りとして設定した実行ＡＣである場合は、この破棄処理をサービス提供処理に続いて実行する。

ステップＳ５７７のＳＣ（セキュリティチップ）登録鍵破棄処理について、図６８を参照して説明する。登録鍵のリセット処理は、共通鍵メモリ領域６０８の登録鍵の格納領域にリセット鍵（Ｋｒｅｓｅｔ）を上書きすることによって行われる。破棄対象となる登録鍵（Ｋｃｒ）のメモリ領域ブロックアドレス（Ａｄ）とリセット鍵（Ｋｒｅｓｅｔ）とからなるリセット処理命令６１７が例えばエンドエンティテイ（ＥＥ）から入力されると、ステップＳ５８３において、リセット処理命令６１７に格納されたメモリ領域ブロックアドレス（Ａｄ）に対応するメモリ領域に、リセット鍵（Ｋｒｅｓｅｔ）の書き込み処理が実行され、登録鍵の削除が完了する。

図６６のシーケンス図に戻り説明を続ける。ステップＳ５７７において、登

録鍵の破棄が完了すると、ステップＳ５７８において登録鍵破棄通知がエンドエンティテイ（ＥＥ）に出力され、エンドエンティテイ（ＥＥ）は、ステップＳ５７９において、実行ＡＣテーブルに対してサービス提供実行ＡＣの削除要求を出力し、実行ＡＣテーブル（制御部）は、実行ＡＣテーブルから対応する実行ＡＣを削除する。

（６－４）登録鍵リセット処理

なお、登録鍵の破棄処理は、サービス提供実行ＡＣの提供処理に続いて実行されるとは限らず、任意タイミングのリセット要求に基づいて登録鍵の破棄処理としてのリセット処理を実行することが可能である。このリセット要求に基づく処理について、図６９を参照して説明する。

ステップＳ６０１において、ユーザがエンドエンティテイ（ＥＥ）のユーザインタフェースを介してユーザデバイスに格納されているサービス提供実行ＡＣに対応する登録鍵のリセット要求を入力する。エンドエンティテイ（ＥＥ）は、ステップＳ６０２において、実行ＡＣテーブルに検索要求を出力する。リセット要求の態様は２通ある。第１の態様は、ユーザが実行ＡＣテーブルのあるメモリ領域ブロックアドレスに書き込んだサービス内容を忘れた場合、メモリ領域ブロックアドレスをキーとして実行ＡＣテーブルを検索し、出力されたＳＰ情報・コンテンツ情報に対応する登録鍵をユーザが不要であると判断するとリセット実行要求を行う態様である。この処理要求には、例えば実行ＡＣの識別子、またはサービス内容を特定するデータ、例えばコンテンツ、プログラム、あるいはサービスプロバイダ（ＳＰ）情報データが含まれる。第２の態様は、ユーザがＳＰ情報・コンテンツ情報を既知の場合、これらをキーとして実行ＡＣテーブルを検索し、出力されたメモリ領域ブロックアドレスをリセット実行要求と共にＳＣへ送信する態様である。なお、登録鍵のメモリ領域ブロックアドレスは、コンテンツ、あるいはサービスプロバイダに対応するデータとしてエンドエンティテイにおいて、任意に格納することが可能である。

ステップＳ６０３において、実行ＡＣテーブルは、エンドエンティテイからの入力キーに基づいて、対応するサービス提供実行ＡＣを検索し、サービス提

供実行ＡＣに対応するサービスプロバイダ、利用可能コンテンツを検索し、ステップＳ６０４において、エンドエンティテイ（ＥＥ）に出力する。

エンドエンティテイ（ＥＥ）では、サービスプロバイダ、利用可能コンテンツ情報を表示し、ユーザが不要であると判定すると、ステップＳ６０６において、セキュリティチップに対してリセット実行要求を出力する。

登録鍵のリセット処理は、共通鍵メモリ領域の登録鍵の格納領域にリセット鍵（Ｋｒｅｓｅｔ）を上書きすることによって行われ、破棄対象となる登録鍵（Ｋｃｒ）のメモリ領域ブロックアドレス（Ａｄ）とリセット鍵（Ｋｒｅｓｅｔ）とからなるリセット処理命令をエンドエンティテイ（ＥＥ）から入力し、ステップＳ６０７において、先に図６８を参照して説明した通りの、メモリ領域ブロックアドレス（Ａｄ）に対応するメモリ領域に、リセット鍵（Ｋｒｅｓｅｔ）の書き込み処理が実行され、登録鍵がリセットされる。ステップＳ６０７において、登録鍵のリセットが完了すると、ステップＳ６０８においてリセット完了通知がエンドエンティテイ（ＥＥ）に出力される。

（６－５）実行属性証明書リセット（破棄）処理

次に、ユーザデバイスに格納された実行属性証明書を破棄し、破棄が間違いなく実行されたことをサービスプロバイダに通知する実行属性証明書リセット（破棄）処理について説明する。

図７０、図７１の処理シーケンス図に従って説明する。図７０、図７１において、

ＥＥ：ユーザデバイスのエンドエンティテイ（ＥＥ）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

実行ＡＣテーブル:実行ＡＣの管理テーブル格納メモリおよびメモリ制御部

ＳＰ：実行ＡＣの発行処理を実行するサービスプロバイダ機器（ＳＰ）制御部、

ＳＭ：ＳＰ内のセキュリティモジュール、

である。

まず、ステップＳ６１１において、ユーザがエンドエンティテイ（ＥＥ）の

入力インタフェースを介して、実行属性証明書（実行ＡＣ）破棄申請要求コマンドを入力する。この要求に基づき、実行属性証明書破棄申請がサービスプロバイダに送信される。申請には、例えば実行属性証明書（実行ＡＣ）ＩＤ、あるいはコンテンツ、サービス指定データ等、破棄対象とする実行属性証明書（実行ＡＣ）を特定可能なデータが含まれる。

サービスプロバイダ機器制御部（ＳＰ）が実行属性証明書破棄申請を受領すると、ステップＳ６１２において、セキュリティチップ（ＳＣ）と、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）間の相互認証、および、必要に応じて実行属性証明書（実行ＡＣ）破棄処理条件として適用されるサービスプロバイダに発行済みのグループ属性証明書の検証、審査処理が行なわれる。実行属性証明書破棄処理をひとつのサービスと見立てた場合、エンドエンティティがサービスプロバイダの役割をになうことになる。

認証処理は、セキュリティチップ、セキュリテイモジュールの暗号処理部（図９参照）を中心とした処理として例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。検証処理は、先に図２１乃至図２３を参照して説明した、属性証明書の署名検証、関連の公開鍵証明書（ＰＫＣ）および連鎖公開鍵証明書の確認処理等を含む処理として実行される。

なお、ここでは、エンドエンティテイ（ＥＥ）のセキュリティチップ（ＳＣ）を発行対象とした実行属性証明書の破棄処理例を示してあるが、ユーザ識別デバイス（ＵＩＤ）のユーザセキュリティチップ（ＵＳＣ）を発行対象とした実行属性証明書の破棄処理の場合は、

（１）ＥＥのＳＣとＳＰ－ＳＭとの相互認証、

（２）ＥＥのＳＣとＵＩＤのＵＳＣとの相互認証、

（３）ＵＩＤのＵＳＣとＳＰ－ＳＭとの相互認証、

のすべてを実行することになる。あるいは、簡便な方式として、ＵＩＤがＥＥに接続されることで、ＥＥは基本的にこれを受け入れる（認証したものとする）という処理構成としてもよく、この場合は、上記（２）の相互認証の省略が可能となる。さらに、上記３種の相互認証の様々な組み合わせによる認証構成が可能である。

ステップＳ６１２の認証、グループ属性証明書の検証、審査がすべて成立すると、ユーザデバイスのエンドエンティテイ（ＥＥ）は、ステップＳ６１３において、破棄対象の実行ＡＣの検索要求を実行ＡＣテーブルに出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ（ＳＰ）情報等である。

ステップＳ６１４において、実行ＡＣテーブルは、エンドエンティテイからの入力キーに基づいて、対応するサービス提供実行ＡＣを検索し、ステップＳ６１５において、テーブルから抽出したサービス提供実行ＡＣをエンドエンティテイ（ＥＥ）に出力する。さらに、実行ＡＣテーブル（制御部）は、ステップＳ６１６において、破棄対象実行ＡＣのエントリを実行ＡＣテーブルから削除する。

ステップＳ６１７において、エンドエンティテイ（ＥＥ）は、セキュリティチップに対してリセット実行要求を出力する。ステップＳ６１８において、登録鍵のリセット処理として、共通鍵メモリ領域の登録鍵の格納領域にリセット鍵（Ｋｒｅｓｅｔ）を上書きする処理（図６８参照）が実行され、リセット完了通知がエンドエンティテイ（ＥＥ）に出力される。

さらに、エンドエンティテイ（ＥＥ）は、図７１に示すステップＳ６２１において、リセット完了通知をサービスプロバイダ（ＳＰ）に送信する。このリセット完了通知は、破棄対象実行ＡＣを伴う。破棄対象実行ＡＣを受領したサービスプロバイダ（ＳＰ）は、ステップＳ６２２において、リセット確認実行ＡＣの生成要求をセキュリティモジュール（ＳＭ）に出力する。この要求は破棄対象実行ＡＣを伴って実行される。

ステップＳ６２３において、セキュリティモジュール（ＳＭ）は、破棄対象の実行ＡＣから、対応する登録鍵を格納したメモリ領域ブロックアドレス情報を抽出し、ステップＳ６２４においてリセット確認実行ＡＣの生成処理を実行する。リセット確認実行ＡＣは、破棄対象の実行ＡＣの対応登録鍵を格納したメモリ領域ブロックアドレス情報（Ａｄ）と、リセット確認実行ＡＣによって、ユーザデバイスのセキュリティチップ（ＳＣ）において実行すべき命令としての実行命令と、発行者、すなわちセキュリティモジュール（ＳＭ）の署名とを含むデータ構成（図７２、リセット確認実行ＡＣ６２１参照）である。

生成されたリセット確認実行ＡＣは、ステップＳ６２５においてサービスプロバイダ（ＳＰ）からエンドエンティテイ（ＥＥ）に送信され、さらに、ステップＳ６２６において、セキュリティチップ（ＳＣ）に転送される。

セキュリティチップ（ＳＣ）では、ステップＳ６２７において、リセット確認実行ＡＣに基づくリセット確認結果生成処理を実行する。ステップＳ６２７のリセット確認結果生成処理の詳細について図７２を参照して説明する。

図７２に示すように、セキュリティチップ６０５は、ステップＳ６４１において、リセット確認実行ＡＣの実行命令を、リセット確認実行ＡＣ６２１に格納されたアドレスに基づいて共通鍵メモリ領域６０８から取り出したリセット鍵（Ｋｒｅｓｅｔ）を適用して復号し、セキュリティチップの公開鍵（ＫｐＳＣ）で暗号化されたデータ（Ｅｐ（ＣｏｎｆＲｅｓｅｔ||Ｋｃｓ；ＫｐＳＣ））の復号命令データ（Ｄｐｃ［Ｅｐ（ＣｏｎｆＲｅｓｅｔ||Ｋｃｓ；ＫｐＳＣ）］を取得し、ステップＳ６４２において、セキュリティチップの秘密鍵（ＫｓＳＣ）を適用して復号し、リセット確認結果作成コマンド（ＣｏｎｆＲｅｓｅｔ）、セッション鍵（Ｋｃｓ）、を取得し、ステップＳ６４３のリセット確認結果作成処理を実行する。

ステップＳ６４３のリセット確認結果作成処理では、まず、ステップＳ６４４において、リセット確認実行ＡＣ６２１に格納されたアドレスに基づいて共通鍵メモリ領域６０８からリセット鍵(Ｋｒｅｓｅｔ)が読み出され、さらに、ステップＳ６４５において、メモリ領域ブロックアドレス情報（Ａｄ）と、リセット鍵(Ｋｒｅｓｅｔ)の連結データをセッション鍵(Ｋｃｓ)で暗号化し、暗号化データ（Ｅｃ（Ａｄ||Ｋｒｅｓｅｔ；Ｋｃｓ））からなるリセット確認結果６２２をエンドエンティテイ（ＥＥ）に出力する。

エンドエンティテイ（ＥＥ）は、図７１のステップＳ６２８においてリセット確認結果をサービスプロバイダ（ＳＰ）に送信し、サービスプロバイダ（ＳＰ）は、ステップＳ６２９においてリセット確認結果をセキュリティモジュール（ＳＭ）に送信し、セキュリティモジュール（ＳＭ）はサービスプロバイダ（ＳＰ）にリセット確認結果通知を送信して処理が終了する。

上述した処理によって、発行済みの実行ＡＣの破棄処理が、サービスプロバ

イダの確認の下に確実に実行されることになる。

なお、登録鍵の破棄処理については、実行ＡＣに基づいて行なうことが可能である。図７３を参照して実行ＡＣに基づく登録鍵の破棄処理について説明する。登録鍵実行ＡＣは、例えば対応するサービス提供実行ＡＣを発行したサービスプロバイダ（ＳＰ）によって発行され、ユーザデバイスのエンドエンティテイ（ＥＥ）を介してセキュリティチップ（ＳＣ）に入力される。

登録鍵破棄実行ＡＣ６２３は、図７３に示すように、破棄対象となる登録鍵を格納した共通鍵メモリ領域のメモリ領域ブロックアドレス情報（Ａｄ）、登録鍵で暗号化した登録鍵破棄コマンド（ＲｅｖＫ）、発行者署名を持つ実行ＡＣである。

ステップＳ６５１において、登録鍵破棄実行ＡＣ６２３のメモリ領域ブロックアドレス情報（Ａｄ）に基づいて、共通鍵メモリ領域６０８から取得した登録鍵(Ｋｃｒ)に基づいて、登録鍵破棄実行ＡＣ６２３の実行命令を復号して、破棄コマンド（ＲｅｖＫ）を取得して、ステップＳ６５２においてコマンドに基づく破棄処理を実行する。ステップＳ６５３では、登録鍵破棄実行ＡＣ６２３のメモリ領域ブロックアドレス情報（Ａｄ）に基づいて、対応メモリ領域にリセット鍵(Ｋｒｅｓｅｔ)が上書きされ、登録鍵が破棄(リセット)される。

[（７）実行属性証明書の具体的利用処理]

次に、上述した実行属性証明書（実行ＡＣ）を適用した具体的な利用処理について説明する。利用処理例として、以下の項目について各々説明する。

（７－１）回数制限付きサービス提供実行属性証明書

（７－２）譲渡機能付きサービス提供実行属性証明書

（７－３）代理発行実行属性証明書

以下、上記項目毎に説明する。

（７－１）回数制限付きサービス提供実行属性証明書

まず、回数制限付きサービス提供実行属性証明書の適用処理について説明する。図７４、図７５に、回数制限付きサービス提供実行属性証明書をユーザデ

バイスにおいて適用してサービス、すなわち、回数制限付き暗号化データ、例えば画像、音楽、プログラム等のコンテンツを復号して利用する処理シーケンスを示す。各ステップに従って処理シーケンスについて説明する。

ユーザデバイスには、すでに回数制限付きサービス提供実行属性証明書がメモリ、例えば前述した実行ＡＣテーブルに格納されており、その残利用回数はｎ回であるものとする。回数制限付きサービス提供実行属性証明書の実行命令中に実行命令の適用可能回数識別値としての残利用回数データ（例えばｎ回）が記録される。記録例については後述する。

ステップＳ７０１において、ユーザがエンドエンティテイ（ＥＥ）のユーザインタフェースを介してサービス提供実行ＡＣ、この例では、暗号化データ復号実行ＡＣの適用処理要求を入力する。この処理要求には、実行ＡＣの識別子、またはサービスプロバイダ（ＳＰ）情報、サービス内容を特定するデータ、例えば利用コンテンツ指定データが含まれる。エンドエンティテイ（ＥＥ）は、ステップＳ７０２において、ユーザ指定のサービス提供実行ＡＣ（暗号化データ復号実行ＡＣ）の検索要求を実行ＡＣテーブルに出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ（ＳＰ）情報等である。

ステップＳ７０３において、実行ＡＣテーブルは、エンドエンティテイからの入力キーに基づいて、対応する暗号化データ復号実行ＡＣを検索し、ステップＳ７０４において、テーブルから抽出した暗号化データ復号実行ＡＣをエンドエンティテイ（ＥＥ）に出力する。この暗号化データ復号実行ＡＣには、残利用回数＝ｎ回の情報が記録されている。

ステップＳ７０４において、エンドエンティテイ（ＥＥ）は、受領ＡＣをセキュリティチップ（ＳＣ）に出力し、サービス提供実行ＡＣ（暗号化データ復号実行ＡＣ）の適用処理要求を行なう。この適用処理は以下のように行なう。まず、ステップＳ７０５において、暗号化データ復号実行ＡＣの実行命令を登録鍵で復号して、復号鍵のセット処理を実行し、復号鍵セット完了通知をエンドエンティテイ（ＥＥ）に出力（Ｓ７０６）し、ＥＥにおいて、例えば外部メモリから復号対象の暗号化データを取得（Ｓ７０７）し、ＳＣに対して復号要求を行ない（Ｓ７０８）、ＳＣにおいてデータ復号処理を実行（Ｓ７０９）し、

復号データをＳＣからＥＥに送信する（Ｓ７１０）データ復号処理を行ない、さらに、ステップＳ７１１において、暗号化データ復号実行ＡＣ中の実行命令中の残利用回数データをｎからｎ－１に更新する。

さらに、更新後の残利用回数の判定（Ｓ７１２）の後、残利用回数≧１の場合は、図７５（ａ）に示すシーケンスに従い、登録鍵の再生成、保存（Ｓ７２１）、暗号化データ復号実行ＡＣの再生成（Ｓ７２２）、ＥＥへの送信、ＥＥからの暗号化データ復号実行ＡＣ保存要求（Ｓ７２３）に応じて、実行ＡＣテーブルへの保存（Ｓ７２４）が実行される。

一方、残利用回数＝０の場合は、図７５（ｂ）に示すシーケンスに従い、ＳＣにおいて、登録鍵の破棄処理（Ｓ７２５）が実行され、ＥＥに対する登録鍵破棄通知（Ｓ７２６）の後、ＥＥからの暗号化データ復号実行ＡＣ削除要求（Ｓ７２７）に応じて、実行ＡＣテーブルの暗号化データ復号実行ＡＣ削除（Ｓ７２８）が実行される。

ステップＳ７０５以下のセキュリティチップ（ＳＣ）における処理を図７６および図７７を参照して説明する。図７６は、更新後の残利用回数≧１の場合の処理であり、図７７は、更新後の残利用回数＝０の場合の処理である。

まず、図７６を参照して、更新後の残利用回数≧１の場合のセキュリティチップ（ＳＣ）における処理について説明する。

回数制限付きサービス提供実行属性証明書７０１は、実行命令（Ｅｃ（ＤｅｃＥＤａｔａ||Ｋｃｄ||ＮｕｍＴｒ（ｎ）；Ｋｃｒ１））と、実行命令を復号する登録鍵を格納した共通鍵メモリ領域におけるブロックアドレス（Ａｄ）と、発行者署名を有する。実行命令には、暗号化データ復号コマンド（ＤｅｃＥＤａｔａ）、データ復号鍵（Ｋｃｄ）、残利用回数（ｎ）に応じた回数処理実行コマンド（ＮｕｍＴｒ（ｎ））が含まれ、登録鍵（Ｋｃｒ１）によってこれらのデータが暗号化された実行命令（Ｅｃ（ＤｅｃＥＤａｔａ||Ｋｃｄ||ＮｕｍＴｒ（ｎ）；Ｋｃｒ１））である。

まず、セキュリティチップ（ＳＣ）は、ステップＳ７３１において、実行ＡＣ中のブロックアドレス（Ａｄ）に基づいて共通鍵メモリ領域から取り出した登録鍵（Ｋｃｒ１）を適用して実行ＡＣ７０１の実行命令を復号し、データ（D

ｅｃＥＤａｔａ||Ｋｃｄ||ＮｕｍＴｒ（ｎ））を取り出して、さらに、ステップＳ７３２において、データ復号鍵（Ｋｃｄ）を適用して、外部から入力される暗号化コンテンツ等の暗号化データ７０２（Ｅｃ（Ｄａｔａ；Ｋｃｄ））の復号を実行して、復号コンテンツ（データ）７０３をエンドエンティティに出力する。

さらに、ステップＳ７３３において、回数処理実行コマンド（ＮｕｍＴｒ（ｎ））に基づく処理を実行する。この処理は、残回数を更新した新たな回数制限付きサービス提供実行属性証明書７０４を生成することを目的とする処理である。

乱数発生処理（Ｓ７３４）により、新たな登録鍵Ｋｃｒ２を生成し、これを元の回数制限付きサービス提供実行属性証明書７０１に書き込まれていたブロックアドレスに対応する共通鍵メモリ領域６０８に書き込む。これにより、先に書き込まれていた登録鍵（Ｋｃｒ１）が新たな登録鍵（Ｋｃｒ２）に置き換えられることになる。

ステップＳ７３６において、回数処理実行コマンド（ＮｕｍＴｒ（ｎ））に基づいて抽出される残利用回数＝ｎをコンテンツの復号処理に伴い（－１）する更新を実行する。すなわち、実行命令中のデータ（ＤｅｃＥＤａｔａ||Ｋｃｄ||ＮｕｍＴｒ（ｎ））を（ＤｅｃＥＤａｔａ||Ｋｃｄ||ＮｕｍＴｒ（ｎ－１））に書き替え、ステップＳ７３７において、新規生成登録鍵（Ｋｃｒ２）を適用した暗号化処理を実行する。この暗号化データは、新たな回数制限付きサービス提供実行属性証明書７０４中の実行命令（Ｅｃ（ＤｅｃＥＤａｔａ||Ｋｃｄ||ＮｕｍＴｒ（ｎ－１）；Ｋｃｒ２））に相当する。

ステップＳ７３８では、ブロックアドレス（Ａｄ）と、ステップＳ７３７において生成した更新した残回数データを持つ実行命令に基づく電子署名をセキュリティチップの秘密鍵（ＫｓＳＣ）によって実行し、新たな更新した回数制限付きサービス提供実行属性証明書７０４を生成する。この場合の署名は、セキュリティチップにおいてなされることになる。

この新たな回数制限付きサービス提供実行属性証明書７０４が、図７５のステップＳ７２２においてセキュリティチップ（ＳＣ）からエンドエンティテイ

（ＥＥ）に出力後、ステップＳ７２４で実行ＡＣテーブルに保存される。

一方、図７４の処理ステップＳ７１２の残利用回数審査において、残利用回数＝０と判定された場合のセキュリティチップ（ＳＣ）における処理を図７７を参照して説明する。

回数制限付きサービス提供実行属性証明書７０５は、実行命令（Ｅｃ（ＤｅｃＥＤａｔａ||Ｋｃｄ||ＮｕｍＴｒ（１）；Ｋｃｒ１））と、実行命令を復号する登録鍵を格納した共通鍵メモリ領域におけるブロックアドレス(Ａｄ)と、発行者署名を有する。

まず、セキュリティチップ（ＳＣ）は、ステップＳ７４１において、実行ＡＣ中のブロックアドレス（Ａｄ）に基づいて共通鍵メモリ領域から取り出した登録鍵(Ｋｃｒ１)を適用して実行ＡＣ７０５の実行命令を復号し、データ(ＤｅｃＥＤａｔａ||Ｋｃｄ||ＮｕｍＴｒ（ｎ))を取り出して、さらに、ステップＳ７４２において、データ復号鍵（Ｋｃｄ）を適用して、外部から入力される暗号化コンテンツ等の暗号化データ７０６Ｅｃ（Ｄａｔａ；Ｋｃｄ))の復号を実行して、復号コンテンツ（データ）７０７をエンドエンティティに出力する。

さらに、ステップＳ７４３において、回数処理実行コマンド（ＮｕｍＴｒ（１))に基づく処理を実行する。この処理は、さらなる実行ＡＣを利用したサービス利用、すなわち暗号化データの復号を停止するため、登録鍵の破棄を実行する処理として行われる。すなわち、ステップＳ７４４において登録鍵(Ｋｃｒ１）の破棄を実行する。登録鍵の破棄は、回数制限付きサービス提供実行属性証明書７０５に記録された登録鍵を格納した共通鍵メモリ領域中のブロックアドレス（Ａｄ）の対応領域にリセット鍵を上書きする処理として実行される。

この処理により、回数制限付きサービス提供実行属性証明書７０５の格納された実行命令を復号する登録鍵（Ｋｃｒ１）が破棄され、実行命令を復号することが不可能になり、実行ＡＣを適用したサービス利用が停止される。この処理の後、図７５に示すステップＳ７２７，Ｓ７２８が実行されて、実行ＡＣテーブルから対応する実行ＡＣが削除される。

（７－２）譲渡機能付きサービス提供実行属性証明書

次に、譲渡機能付きサービス提供実行属性証明書の適用処理について説明する。図７８に、譲渡機能付きサービス提供実行属性証明書の適用処理、すなわち、ユーザデバイス間で譲渡機能付きサービス提供実行属性証明書に基づく処理を実行して、新たな譲渡機能付きサービス提供実行属性証明書、あるいはサービス提供実行ＡＣを生成して他のユーザデバイス（譲渡先）に送付するとともに、自デバイス（譲渡元）の登録鍵を破棄する処理を行なうことで、他のユーザデバイスにおいて暗号化データ（例えば暗号化コンテンツ）を利用することを可能とした処理シーケンスを示す。

図７８において、

ＥＥ１：譲渡元ユーザデバイスのエンドエンティテイ（ＥＥ）制御部、

ＳＣ１：譲渡元ＥＥ内に構成されるセキュリティチップ、

実行ＡＣテーブル１：譲渡元エンドエンティテイ（ＥＥ）実行ＡＣテーブル制御部、

ＥＥ２：譲渡先ユーザデバイスのエンドエンティテイ（ＥＥ）制御部、

ＳＣ２：譲渡先ＥＥ内に構成されるセキュリティチップ、

実行ＡＣテーブル２：譲渡先エンドエンティテイ（ＥＥ）実行ＡＣテーブル制御部、

である。

まず、ステップＳ７５２において、譲渡先のユーザがエンドエンティテイ（ＥＥ２）の入力インタフェースを介して、譲渡機能付きサービス提供実行属性証明書に基づく譲渡処理、すなわち暗号化データの利用を譲渡先ユーザデバイスで実行可能とするための譲渡要求を入力する。譲渡要求には、譲渡機能付きサービス提供実行属性証明書のＩＤ、および所有者情報、あるいは利用コンテンツ（暗号化データ）、あるいはサービスプロバイダ情報等、適用する譲渡機能付きサービス提供実行属性証明書を特定するための情報が含まれる。

エンドエンティテイ（ＥＥ２）がユーザからの譲渡要求の入力を受領すると、エンドエンティテイ（ＥＥ２）は、ステップＳ７５２において、譲渡機能付き

サービス提供実行属性証明書を所有する譲渡元ユーザデバイスのエンドエンティテイ（ＥＥ１）に対する接続要求を行ない、各ユーザデバイスのセキュリティチップ（ＳＣ１）、（ＳＣ２）間において相互認証を実行する。これは例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。

相互認証が成立すると、ステップＳ７５３において、譲渡元のユーザデバイスのエンドエンティテイ（ＥＥ１）は、指定された譲渡機能付きサービス提供実行属性証明書の検索要求を実行ＡＣテーブル１に出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ（ＳＰ）情報等である。

ステップＳ７５４において、実行ＡＣテーブル１は、エンドエンティテイ（ＥＥ１）からの入力キーに基づいて、対応する譲渡機能付きサービス提供実行属性証明書を検索し、テーブルから抽出した実行ＡＣをエンドエンティテイ（ＥＥ）に出力する。

ステップＳ７５５において、エンドエンティテイ（ＥＥ）は、受領ＡＣをセキュリティチップ（ＳＣ）に出力し、譲渡機能付きサービス提供実行属性証明書の適用処理要求を行なう。セキュリティチップは、ステップＳ７５６において、受領ＡＣの処理、すなわち、実行属性証明書（譲渡機能付きサービス提供実行属性証明書）に格納されたアドレス（Ａｄ）によって指定された領域から取得される登録鍵に基づく実行命令の復号（Ｓ７５６）を行なう。

さらに、ステップＳ７５７において、エンドエンティテイ（ＥＥ１）から譲渡処理要求がセキュリティチップ（ＳＣ）に出力し、エンドエンティテイ（ＥＥ１）はステップＳ７５８において、譲渡処理のために必要とするグループ属性証明書の提示を譲渡先のユーザデバイス（ＥＥ２）に対して要求する。このグループ属性証明書は、例えば、譲渡機能付きサービス提供実行属性証明書を生成発行したサービスプロバイダ（ＳＰ）によって管理された譲渡可能ユーザデバイスあるいはユーザのグループであることを証明するグループ属性証明書等である。

譲渡先ユーザデバイスのエンドエンティテイ（ＥＥ２）は、ステップＳ７５９において、指定のグループ属性証明書（Ｇｐ．ＡＣ）を譲渡元ユーザデバイ

スのエンドエンティテイ（ＥＥ１）に送信し、エンドエンティテイ（ＥＥ１）は、受領ＡＣをセキュリティチップ（ＳＣ１）に転送し、セキュリティチップ（ＳＣ１）が、グループ属性証明書を検証する（Ｓ７６１）。この検証処理は、先に図２１～図２３を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。

検証不成立の場合は、エラー処理として、その後の処理を実行せず処理を中止する。この場合、エラー通知を譲渡先エンドエンティテイ（ＥＥ２）に送信する処理を行なってもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ７６２に進む。ステップＳ７６２では、譲渡先ユーザデバイスにおいて暗号化データの利用を可能とするための実行属性証明書の生成、送信が行なわれることになる。これらの処理は、先に図６０、図６１を参照して説明した登録鍵生成実行ＡＣの生成、検証、サービス提供実行ＡＣの生成送信に対応する処理であり、図６０、図６１におけるサービスプロバイダ（ＳＰ）の処理を譲渡元ユーザデバイスが実行するものである。

ステップＳ７６２において、新たなサービス提供実行ＡＣ、この例では、サービス提供実行属性証明書が生成されて、譲渡先ユーザデバイスに送付される。さらに、ステップＳ７６３において、譲渡元ユーザデバイスが保有していた譲渡機能付きサービス提供実行属性証明書の実行命令を復号するために適用する登録鍵の削除が実行される。この処理は、前述したリセット鍵の上書きによって行なわれるものである。なおここでは、譲渡の機能について述べたが、登録鍵の削除を行わない実行属性証明書を用いれば、譲渡ではなく複製の機能を持たせることが出来る。

譲渡元ユーザデバイスのセキュリティチップ（ＳＣ１）で実行するステップＳ７５６の譲渡機能付きサービス提供実行属性証明書の復号処理以下の処理の詳細について、図７９、図８０を参照して説明する。

譲渡機能付きサービス提供実行属性証明書（ＡＣ）７１１には、実行命令、実行命令を復号するための登録鍵を格納した共通鍵メモリ領域６０８のプロ

ックアドレス（Ａｄ１）、発行者署名の各データを有する。実行命令（Ｅｃ（Ｓｅｌ||Ｊｄｇ（ＳＤＢ）||ＧｅｎＡＣ（ＧｅｎＫｃｒ）||ＧｅｎＡＣ（Ｅｘ）||ＲｅｖＫ||ＤｅｃＥＤａｔａ||Ｋｃｄ；Ｋｃｒ１））には、処理選択コマンド（Ｓｅｌ）、検証審査コマンド（Ｊｄｇ（ＳＤＢ））、登録鍵生成実行ＡＣ作成コマンド（ＧｅｎＡＣ（ＧｅｎＫｃｒ）、実行ＡＣ作成コマンド（ＧｅｎＡＣ（Ｅｘ）、登録鍵破棄コマンド（ＲｅｖＫ）、暗号化データ復号コマンド（ＤｅｃＥＤａｔａ）、データ復号鍵（Ｋｃｄ）が含まれ、これらを登録鍵（Ｋｃｒ１）で暗号化したデータ構成である。

なお、検証審査コマンド（Ｊｄｇ（ＳＤＢ））は、サービス情報データベース（ＳＤＢ）に基づく実行ＡＣの検証審査処理コマンドである。なお、サービス情報データベース（ＳＤＢ）は、サービス提供に必要となるＡＣ情報、および先に説明したグループ情報データベース（図１５参照）と同様のデータ構成を持ち、発行者、グループＩＤ、グループ情報の各データを有する。

譲渡機能付きサービス提供実行属性証明書（ＡＣ）７１１を入力して、譲渡先に新たな譲渡機能付きサービス提供実行属性証明書を発行する処理を実行する譲渡元セキュリテイチップ（ＳＣ）は、まず、譲渡機能付きサービス提供実行属性証明書（ＡＣ）７１１のアドレス（Ａｄ１）に基づいて共通鍵メモリ領域６０８から登録鍵を取得し、譲渡機能付きサービス提供実行属性証明書（ＡＣ）７１１内の実行命令を復号する。次に、譲渡実行トリガ７１２をエンドエンティテイから入力すると、ステップＳ７７２以下の譲渡実行処理を行なう。

ここで、譲渡実行トリガ７１２は、譲渡機能付きサービス提供実行属性証明書（ＡＣ）７１１に基づく、譲渡処理を実行することのエンドエンティテイからの要求処理を示す。譲渡機能付きサービス提供実行属性証明書（ＡＣ）７１１は、譲渡処理のみならず、暗号化データの復号処理の際にも適用される実行ＡＣであり、そのいずれの処理を実行するかをエンドエンティテイからの要求（トリガ）によって選択する。譲渡機能付きサービス提供実行属性証明書（ＡＣ）７１１の実行命令（Ｅｃ（Ｓｅｌ||Ｊｄｇ（ＳＤＢ）||ＧｅｎＡＣ（ＧｅｎＫｃｒ）||ＧｅｎＡＣ（Ｅｘ）||ＲｅｖＫ||ＤｅｃＥＤａｔａ||Ｋｃｄ；

Ｋｃｒ１））から選択処理によって、譲渡実行処理に対応する実行命令（Ｊｄｇ（ＳＤＢ）||ＧｅｎＡＣ（ＧｅｎＫｃｒ）||ＧｅｎＡＣ（Ｅｘ）||ＲｅｖＫ）が取得され、ステップＳ７７２以下の処理を実行命令に従って実行する。

ステップＳ７７２では、検証審査コマンド（Ｊｄｇ（ＳＤＢ））に従って、譲渡先から取得したグループ属性証明書（Ｇｐ．ＡＣ）７１３の検証、審査を行なう。この検証処理は、先に図２１～図２３を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。検証不成立の場合は、エラー処理として、その後の処理を実行せず処理を中止する。グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ７７３に進む。

ステップＳ７７３以下では、譲渡先ユーザデバイスにおいて暗号化データの利用を可能とするための実行属性証明書の生成、送信が行なわれることになる。これらの処理は、先に図６０、図６１、図６３～図６５を参照して説明した登録鍵生成実行ＡＣの生成、検証、サービス提供実行ＡＣの生成送信に対応する処理であり、図６０、図６１におけるサービスプロバイダ（ＳＰ）の処理を譲渡元ユーザデバイスが実行するものである。

これらの処理に必要なリセット鍵（Ｋｒｅｓｅｔ）、譲渡先の共通鍵メモリの登録鍵格納領域のブロックアドレス（Ａｄ２）、譲渡先のセキュリティチップの公開鍵（ＫｐＳＣ２）等のデータ７１４は、譲渡先のユーザデバイス等から取得する。これらの必要データに基づいて、まず、ステップＳ７７３において、実行命令中の登録鍵生成実行ＡＣ作成コマンド（ＧｅｎＡＣ（ＧｅｎＫｃｒ）に従って、登録鍵生成実行ＡＣ７１５の生成処理がなされる。この処理は、先に図６３を参照して説明した登録鍵生成実行ＡＣの生成処理と同様である。

次に、譲渡元ユーザデバイスのセキュリティチップから、登録鍵生成実行ＡＣを受信した譲渡先ユーザデバイスのセキュリティチップは、実行命令中の実行ＡＣ作成コマンド（ＧｅｎＡＣ（Ｅｘ）に従い、先に図６４を参照して説明した処理に従って、登録鍵生成実行結果（図８０，７２１）を生成して譲渡元ユーザデバイスのセキュリティチップに送信する。

譲渡先ユーザデバイスのセキュリティチップから、登録鍵生成実行結果（図８０，７２１）を受信した譲渡元ユーザデバイスのセキュリティチップは、図８０に従った処理を行なって、新たな譲渡機能付きサービス提供実行属性証明書（ＡＣ）７２２を生成して譲渡先ユーザデバイスに送信するとともに、自己の共通鍵メモリ領域中の登録鍵を破棄する処理を実行する。

図８０のステップＳ７８１において、セッション鍵（Ｋｃｓ）を適用して、登録鍵生成結果の復号処理を実行し、登録鍵（Ｋｃｒ２）とメモリ領域ブロックアドレス（Ａｄ２）を取得する。さらに、ステップＳ７８２において、新たな譲渡機能付きサービス提供実行属性証明書（ＡＣ）７２２に格納する実行命令（Ｅｃ（Ｓｅｌ||Ｊｄｇ（ＳＤＢ）||ＧｅｎＡＣ（ＧｅｎＫｃｒ）||ＧｅｎＡＣ（Ｅｘ）||ＲｅｖＫ||ＤｅｃＥＤａｔａ||Ｋｃｄ；Ｋｃｒ２））を、譲渡先ユーザデバイスの登録鍵（Ｋｃｒ２）を適用して暗号化する。なお、実行命令は、サービス提供実行ＡＣとしての新たな譲渡機能付きサービス提供実行属性証明書（ＡＣ）７２２に設定される実行プログラム等の実行命令である。

さらに、ステップＳ７８３において、実行命令を登録鍵（Ｋｃｒ２）で暗号化したデータと、登録鍵（Ｋｃｒ２）を格納する譲渡先ユーザデバイスにおけるセキュリティチップのメモリ領域ブロックアドレス（Ａｄ２）とのデータに対して、譲渡元のセキュリティチップ（ＳＣ１）の秘密鍵（ＫｓＳＣ１）によって署名（図１７参照）が生成され、新たな譲渡機能付きサービス提供実行属性証明書（ＡＣ）７２２が生成されて、譲渡先ユーザデバイスに送信される。

さらに、ステップＳ７８４では、元の譲渡機能付きサービス提供実行属性証明書（ＡＣ）７１１に格納されたアドレス（Ａｄ１）、すなわち、譲渡元のユーザデバイスの共通鍵メモリ領域の登録鍵格納アドレスに対するリセット鍵の書き込みが実行されて、登録鍵の破棄処理が実行される。

なお、上記説明では、譲渡元から譲渡先に対して新たな譲渡機能付きサービス提供実行属性証明書（ＡＣ）７２２を生成して送付する構成例を示したが、新たな譲渡機能付きサービス提供実行属性証明書（ＡＣ）７２２ではなく、通常の、すなわち譲渡機能を持たないサービス提供実行属性証明書（ＡＣ）を生成して送付する構成としてもよい。

譲渡機能付きサービス提供実行属性証明書(ＡＣ)は、先に説明したように、譲渡処理のみならず、暗号化データの復号処理の際にも適用される実行ＡＣである。そのいずれの処理を実行するかをエンドエンティテイからの要求(トリガ)によって選択する。トリガが暗号化データの復号処理の要求である場合のセキュリティチップにおける処理を図８１を参照して説明する。

譲渡機能付きサービス提供実行属性証明書（ＡＣ）７３１には、実行命令、実行命令を復号するための登録鍵を格納した共通鍵メモリ領域６０８のブロックアドレス（Ａｄ１）、発行者署名の各データを有する。

譲渡機能付きサービス提供実行属性証明書（ＡＣ）７３１を入力したセキュリテイチップ(ＳＣ)は、まず、譲渡機能付きサービス提供実行属性証明書(ＡＣ)７３１のアドレス（Ａｄ１）に基づいて共通鍵メモリ領域６０８から登録鍵を取得し、譲渡機能付きサービス提供実行属性証明書（ＡＣ）７３１内の実行命令を復号する。次に、暗号化データ復号トリガ７３２をエンドエンティテイから入力すると、ステップＳ７８６において、トリガに基づく選択処理、すなわち、データ復号実行の選択を行ない、ステップＳ７８７において、復号処理を実行する。

すなわち、譲渡機能付きサービス提供実行属性証明書（ＡＣ）７３１の実行命令（Ｅｃ（Ｓｅｌ||Ｊｄｇ（ＳＤＢ）||ＧｅｎＡＣ（ＧｅｎＫｃｒ）||ＧｅｎＡＣ（Ｅｘ）||ＲｅｖＫ||ＤｅｃＥＤａｔａ||Ｋｃｄ；Ｋｃｒ１））から選択処理によって、データ復号処理に対応する実行命令（ＤｅｃＥＤａｔａ||Ｋｃｄ）が取得され、ステップＳ７８７において、データ復号鍵（Ｋｃｄ）を適用して、外部から入力される復号対象の暗号化データ（Ｅｃ（Ｄａｔａ；Ｋｃｄ））７３３の復号処理を実行し、復号されたデータ７３４を出力する。復号対象の暗号化データ（Ｅｃ（Ｄａｔａ；Ｋｃｄ））７３３は、例えば画像、音楽、プログラム等のコンテンツを、鍵（Ｋｃｄ）により暗号化したデータであり、譲渡機能付きサービス提供実行属性証明書（ＡＣ）７３１内の格納実行命令を登録鍵（Ｋｃｒ１）によって復号することによって取得可能なデータ復号鍵（Ｋｃｄ）によって復号可能となる。

譲渡機能と回数制限を組み合わせた適用例も考えられる。例えば、譲渡され

る実行ＡＣは、譲渡を行う実行ＡＣの回数情報が一つ減ったものとなるように設定すれば、移動回数を制限できる。また、複製機能と回数制限を組み合わせた適用例も考えられる。例えば、複製を行うたびに実行属性証明書の回数情報が一つ減ったものとなるように設定すれば、複製回数を制限できる。ここで、複製というのは、複製機能を持たないサービス提供実行属性証明書に対して行う。さらに、一旦複製したサービス提供実行属性証明書を破棄する代わりに、回数情報を一つ増える機能を持たせれば、チェックイン・チェックアウト機能が実現できる。

チェックイン・チェックアウトについて簡単に説明する。サービス利用権限を他の機器に転送することをチェックアウトといい、さらにチェックアウトした機器から元の機器に転送することをチェックインという。サービス利用権限がチェックアウトした機器から元の機器以外に転送することの出来ない時、チェックイン・チェックアウト機能を持つという。

（７－３）代理発行実行属性証明書

次に代理発行実行属性証明書について説明する。（６－３）実行属性証明書適用処理では、コンテンツを暗号化したデータの復号サービスについて述べたが、サービスプロバイダしか知らない暗号鍵を実行属性証明書に書き込み、その暗号鍵を使って署名付けした証明書を発行するサービスも実行属性証明書を用いて行うことが出来る。このサービス提供実行属性証明書が代理発行実行属性証明書である。

この暗号鍵として、共通鍵を用いる方法と秘密鍵を用いる方法がある。以下では、秘密鍵を用いる場合について述べる。代理発行実行属性証明書を用いて発行する証明書を検証するには、検証者は、上記秘密鍵に対応した公開鍵を知る必要がある。そのため、代理発行実行属性証明書発行者は、上記公開鍵の証明書を発行し、代理発行実行属性証明書を用いて発行する証明書所有者は、検証者に、上記公開鍵証明書を提示する。この公開鍵証明書を代理署名鍵証明書と呼ぶ。この代理発行実行属性証明書として、以下の項目について各々説明する。

（７－３－１）審査代行実行属性証明書

（７－３－２）代理署名実行属性証明書

以下、上記項目ごとに説明する。

（７－３－１）審査代行実行属性証明書

まず、審査代行実行属性証明書について説明する。属性証明書登録局が、直接情報をやり取りするのが難しいエンドエンティティに属性証明書を発行する際、発行ポリシーを規定した状態で、予め属性証明書登録局が直接情報をやり取りすることの出来る別のエンドエンティティに、発行の審査を代行させることを可能とさせるのが、審査代行実行属性証明書である。

図８２を参照して審査代行実行属性証明書の概要を説明する。図８２（ａ）は、通常の属性証明書の発行形態を示し、属性証明書（ＡＣ）の利用者である属性保持者から例えば属性認証局（ＡＡ）、属性証明書登録局（ＡＲＡ）あるいはサービスプロバイダ（ＳＰ）等の発行者に対して属性証明書、ここではグループ属性証明書（Ｇｐ．ＡＣ）の発行要求（Ｓ８０１）を行なう。例えばこの場合、ＡＣ利用者の属性を証明するデータの提出が必要となる。前述した実施例では、例えばクレジットカード会社がすでにＡＣ利用者に対して発行済みのグループ属性証明書の提示をする例を説明した。

発行者は、ＡＣ利用者の属性等のユーザ確認としての審査を実行（Ｓ８０２）して、審査成立と判定すると、ＡＣ利用者の属性を証明する属性証明書（ここではＧｐ．ＡＣ）８０１を利用者に発行（Ｓ８０３）する。

（ｂ）に示す例は、以下において詳細に説明する審査代行実行属性証明書を適用したグループ属性証明書（Ｇｐ．ＡＣ）発行シーケンスである。

まず、ＡＣ利用者に対してグループ属性証明書を代理発行する審査代行者が、本来の発行者、例えば属性認証局（ＡＡ）、属性証明書登録局（ＡＲＡ）あるいはサービスプロバイダ（ＳＰ）に対して、審査代行実行属性証明書の発行要求（Ｓ８１１）を行ない、真の発行者である属性認証局（ＡＡ）、属性証明書登録局（ＡＲＡ）あるいはサービスプロバイダ（ＳＰ）等が、審査代行者の審査（Ｓ８１２）を行なう。これは、従来と同様、審査代行者の属性等を証明す

るデータ、あるいは既発行の属性証明書の提示等に基づいて実行する。審査成立後、発行者は、代理署名鍵証明書８０４と、審査代行実行属性証明書８０３を審査代行者に付与（Ｓ８１３）する。

代理署名鍵証明書８０４は、代理署名生成、検証の際に用いる公開鍵（Ｋｐａ）と、発行者署名データを有する。また、審査代行実行属性証明書８０３は、前述の実行証明書と同様、審査代行者のユーザデバイスの共通鍵メモリの登録鍵（Ｋｃｒ）の格納領域を示すブロックアドレス（Ａｄ）、登録鍵（Ｋｃｒ）で暗号化された実行命令（Ｅｃ（代行審査命令||属性情報||Ｋｓａ；Ｋｃｒ））、発行者署名からなる。

実行命令に含まれる秘密鍵（Ｋｓａ）は、代理署名生成、検証の際に用いる秘密鍵であり、前述の公開鍵（Ｋｐａ）に対応する秘密鍵である。

ステップＳ８１１～Ｓ８１３は、代行委託フェーズであり、この代行委託フェーズの完了の後、代行実行フェーズが開始される。ＡＣ利用者（属性保持者）から、属性証明書（Ｇｐ．ＡＣ）の発行要求が審査代行者になされる（Ｓ８１４）。ここでは、審査代行者の発行するグループ属性証明書を審査代行グループ属性証明書と呼ぶ。

審査代行グループ属性証明書の発行要求を受領した審査代行者は、利用者の審査（Ｓ８１５）を行なう。ここでの審査は、審査代行者とＡＣ利用者との信頼関係に基づいて実行することも可能であり、審査代行者の属性等を証明するデータ、あるいは既発行の属性証明書の提示等を必ずしも必要としない。例えば審査代行者をある家族の１人とし、利用者をその家族とする設定であれば、審査代行者が家族であることを認定すれば、審査成立とする等、審査代行者とＡＣ利用者との信頼関係に基づいて任意の審査を行なうことが可能である。

審査成立の後、審査代行者は、審査代行グループ属性証明書８０２を生成する。審査代行グループ属性証明書８０２は、ＡＣ利用者（属性保持者）のセキュリティチップに対して発行された公開鍵証明書（ＰＫＣ）シリアル番号、属性情報等、先に図５を参照して説明した各情報を持つ。さらに、先に、審査代行者が発行者から受領した審査代行実行属性証明書８０２の実行命令中に格納された秘密鍵（Ｋｓａ）を適用した署名が付加される。

審査代行者は、生成した審査代行グループ属性証明書８０２と、代理署名鍵証明書８０４を併せてＡＣ利用者に送付（Ｓ８１６）する。ＡＣ利用者は、審査代行グループ属性証明書８０２を、例えばサービスプロバイダ（ＳＰ）に提示して属性を証明してサービスを受領する。

サービス提供も含めた各エンティテイ間でのデータの流れを図８３を参照して説明する。まず、代行委託フェーズにおいて、発行者８１１から審査代行実行ＡＣ８２２、代理署名鍵証明書８２１が審査代行者８１２に送付される。次に、代行実行フェーズにおいて、審査代行グループ属性証明書８２３と、代理署名鍵証明書８２１がＡＣ利用者（属性所有者）８１３に送付される。さらに、サービスプロバイダ（ＳＰ）等の検証者８１４に対して、審査代行グループ属性証明書８２３と、代理署名鍵証明書８２１がＡＣ利用者（属性所有者）８１３から送付され、検証者８１４が、審査代行グループ属性証明書８２３と、代理署名鍵証明書８２１に基づくＡＣ利用者の属性検証を実行し、検証成立を条件としてサービスを提供する。

サービスプロバイダ（ＳＰ）等の検証者８１４は、代理署名鍵証明書８２１の署名検証の後、代理署名鍵証明書８２１に格納された代理署名検証用の公開鍵（Ｋｐａ）を取り出して、取り出した公開鍵（Ｋｐａ）を適用して、審査代行グループ属性証明書８２３の署名検証を実行することができる。

次に、発行者から審査代行実行ＡＣ８２２、代理署名鍵証明書８２１を受領した審査代行者がＡＣ利用者の要求に基づいて、審査代行グループ属性証明書８２３を生成、発行する処理について、図８４を参照して説明する。図８４において、

ＥＥ１：属性証明書利用ユーザデバイスのエンドエンティテイ（ＥＥ）制御部、

ＳＣ１：ＥＥ１内に構成されるセキュリティチップ、

ＥＥ２：審査代行者ユーザデバイスのエンドエンティテイ（ＥＥ）制御部、

ＳＣ２：ＥＥ２内に構成されるセキュリティチップ、

実行ＡＣテーブル：ＥＥ２の実行ＡＣテーブル制御部、

である。

なお、審査代行者は、ユーザデバイスに限らず、例えばサービスプロバイダ（ＳＰ）が実行する構成も可能である。ここでは一例としてユーザデバイスが審査代行者として機能する例を説明する。

まず、ステップＳ８２１において、ＡＣ利用者（属性所有者）としてのユーザがエンドエンティテイ（ＥＥ１）の入力インタフェースを介して、審査代行グループ属性証明書（Ｇｐ．ＡＣ）の発行要求を入力する。要求には、審査代行者の指定データ、および利用予定のコンテンツあるいはサービスプロバイダ情報等、審査代行グループ属性証明書（Ｇｐ．ＡＣ）の生成に必要となる情報を含む。

エンドエンティテイ（ＥＥ１）がユーザからの審査代行グループ属性証明書（Ｇｐ．ＡＣ）の発行要求を受領すると、エンドエンティテイ（ＥＥ１）は、ステップＳ８２２において、審査代行者のユーザデバイスのエンドエンティテイ（ＥＥ２）に対する接続要求を行ない、各ユーザデバイスのセキュリティチップ（ＳＣ１）、（ＳＣ２）間において相互認証を実行する。これは例えば先に図１３を参照して説明した公開鍵方式の相互認証処理として実行される。

相互認証が成立すると、ステップＳ８２３において、審査代行者ユーザデバイスのエンドエンティテイ（ＥＥ２）は、審査代行実行ＡＣの検索要求を実行ＡＣテーブルに出力する。検索キーは、例えばコンテンツ情報やサービスプロバイダ（ＳＰ）情報等である。

ステップＳ８２４において、実行ＡＣテーブルは、エンドエンティテイ（ＥＥ２）からの入力キーに基づいて、対応する審査代行実行ＡＣを検索し、テーブルから抽出した実行ＡＣとそのＡＣに付帯して発行者から発行された代理署名鍵証明書（図８２，８０４参照）をエンドエンティテイ（ＥＥ２）に出力する。

ステップＳ８２５において、エンドエンティテイ（ＥＥ２）は、受領ＡＣをセキュリティチップ（ＳＣ２）に出力し、実行属性証明書の適用処理要求を行なう。セキュリティチップ（ＳＣ２）は、ステップＳ８２６において、受領ＡＣの処理、すなわち、実行属性証明書（審査代行実行ＡＣ）に格納されたアドレス（Ａｄ）によって指定された領域から取得される登録鍵に基づく実行命令

の復号を行なう。

さらに、ステップＳ８２７において、ＡＣ利用者の審査のためのグループ属性証明書がＡＣ利用者のエンドエンティテイ（ＥＥ１）から審査代行者のエンドエンティテイ（ＥＥ２）に入力され、審査代行者のセキュリティチップ（ＳＣ２）において検証処理が実行される。

前述したように、審査代行者は、ＡＣ利用者の審査を審査代行者とＡＣ利用者との信頼関係に基づいて実行可能であり、審査代行者の属性等を証明するデータ、あるいは既発行の属性証明書の提示等を必ずしも必要としないが、ここでは、既発行のグループ属性証明書の提示、検証を条件として審査代行グループ属性証明書を発行する例を示している。

セキュリティチップ（ＳＣ２）によるグループ属性証明書の検証は、先に図２１～図２３を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。検証不成立の場合は、エラー処理として、その後の処理を実行せず処理を中止する。この場合、エラー通知をＡＣ利用者エンドエンティテイ（ＥＥ１）に送信する処理を行なってもよい。

グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ８３０において、審査代行グループ属性証明書の生成に必要とする追加情報（Ａｄｄｉｎｆｏ）をエンドエンティテイ（ＥＥ２）からセキュリティチップ（ＳＣ２）に入力し、セキュリティチップ（ＳＣ２）は審査代行グループ属性証明書を生成し、エンドエンティテイ（ＥＥ２）に送付の後、エンドエンティテイ（ＥＥ２）からＡＣ利用者のエンドエンティテイ（ＥＥ１）に送付（Ｓ８３２）される。この送付処理に際しては、生成した審査代行グループ属性証明書に代理署名鍵証明書を付加して送付する。

審査代行者のセキュリティチップ（ＳＣ２）で実行する処理、すなわち審査代行実行属性証明書を入力して審査代行グループ属性証明書を生成する処理の詳細を図８５を参照して説明する。審査代行実行属性証明書（ＡＣ）８５１には、実行命令、実行命令を復号するための登録鍵（Ｋｃｒ）を格納した審査

代行者セキュリティチップ（ＳＣ）８６１の共通鍵メモリ領域８６４のブロックアドレス（Ａｄ）、発行者署名の各データを有する。実行命令（Ｅｃ（Ｊｄｇ（ＳＤＢ）||ＧｅｎＡＣ（Ｇｐ）||ａｔｔ||Ｋｓａ；Ｋｃｒ））には、検証審査コマンド（Ｊｄｇ（ＳＤＢ））、グループ属性証明書作成コマンド（ＧｅｎＡＣ（Ｇｐ）、属性情報（ａｔｔ）、代理署名用秘密鍵（Ｋｓａ）が含まれ、これらを登録鍵（Ｋｃｒ）で暗号化したデータ構成である。

審査代行実行属性証明書（ＡＣ）８５１を入力すると、まず、審査代行実行属性証明書（ＡＣ）８５１のアドレス（Ａｄ）に基づいて共通鍵メモリ領域８６４から登録鍵を取得し、審査代行実行属性証明書（ＡＣ）８５１内の実行命令を復号する。次に、ステップＳ８４２において、検証審査コマンド（Ｊｄｇ（ＳＤＢ））に基づいて、ＡＣ利用者からエンドエンティテイを介して入力するグループ属性証明書の検証を実行する。この検証処理は、先に図２１～図２３を参照して説明したと同様の処理であり、属性証明書の署名検証、対応および連鎖公開鍵証明書の検証等を含む処理である。検証不成立の場合は、エラー処理として、その後の処理を実行せず処理を中止する。グループ属性証明書（Ｇｐ．ＡＣ）の検証が成功し、グループ属性証明書（Ｇｐ．ＡＣ）の正当性が確認されるとステップＳ８４３に進む。

ステップＳ８４３では、審査代行実行ＡＣ８５１内の実行命令中のグループ属性証明書作成コマンド（ＧｅｎＡＣ（Ｇｐ））に基づいて、審査代行グループ属性証明書の生成、送信が行なわれることになる。これらの処理は、先に図６０、図６１、図６３～図６５を参照して説明した登録鍵生成実行ＡＣの生成、検証、サービス提供実行ＡＣの生成送信に対応する処理であり、図６３～図６５におけるサービスプロバイダ（ＳＰ）のセキュリテイモジュールにおける処理と同様である。なお、例えば審査代行属性証明書であることを示す追加情報（ａｄｄｉｎｆｏ）８５３を審査代行属性証明書に付加して、通常の属性証明書と異なることを示すものとすることが好ましい。

ステップＳ８４４では、審査代行実行属性証明書（ＡＣ）８５１の実行命令中から取得した代理署名用の秘密鍵（Ｋｓａ）を適用して、追加情報（ａｄｄｉｎｆｏ）および属性情報（ａｔｔ）に対する署名を行ない、審査代行グルー

プ属性証明書８５４を生成し、エンドエンティテイ（ＥＥ２）を介してＡＣ利用者（属性所有者）に送信する。なお、ＡＣ利用者には、生成した審査代行グループ属性証明書に代理署名鍵証明書を付加して送付する。

ＡＣ利用者は、上述の処理によって発行された審査代行グループ属性証明書と、代理署名鍵証明書を、サービスプロバイダ等の検証者に提示して、属性検証を条件としたサービスを受領することになる。サービスプロバイダ等の検証者は、代理署名鍵証明書から取得可能な鍵を適用して審査代行グループ属性証明書の署名検証が可能となる。

上述した審査代行グループ属性証明書の適用例としては、例えばアカウント数を制限した審査代行グループ属性証明書の発行例がある。サービスプロバイダ（ＳＰ）がＡさんの家族全員にサービスを提供する時に、Ａさんの家族であるかどうかＡ家の家族であることを証明するグループ属性証明書（Ｇｐ．ＡＣ）を用いて審査するとする。

このとき、Ａ家の家族であることを証明するグループ属性証明書（Ｇｐ．ＡＣ）として、役所など住民の基本情報を持った第三者機関が発行した属性証明書（ＡＣ）を用いることができれば、信頼性の高い属性審査が可能となるが、このような属性証明書が利用可能な状態にあるとは限らない。一方、Ａさん自身にＡ家の家族であることを証明するグループ属性証明書（ＧｐＡＣ）を発行させることはＡさんの意思に応じて可能となる。しかし、属性証明書の真の発行主体である属性認証局（ＡＡ）としてＡさん等の個人を信頼できると判定することは難しい。

そこで、上述した審査代行実行ＡＣを適用した審査代行グループ属性証明書を発行する。この場合、Ａさんの家族の代表者としてのＡさんが審査代行者として、審査代行実行ＡＣを適用した審査代行グループ属性証明書の発行を行なう。この時の審査代行グループ属性証明書の発行審査は、審査代行者（Ａさん）とＡＣ利用者（Ａさんの家族）との信頼関係に基づいて実行することが可能であり、審査代行者の属性等を証明するデータ、あるいは既発行の属性証明書の提示等を必ずしも必要としない。審査代行者が家族であることを認定すれば、審査成立とする等、審査代行者とＡＣ利用者との信頼関係に基づいて審査代行

グループ属性証明書を発行することが可能である。

ただし、Aさんは、本当は家族でない友人のBさんにもAさんの家族であることを属性として示す審査代行グループ属性証明書を発行してしまうかもしれない。このような可能性を抑えるため、審査代行グループ属性証明書の発行枚数に制限、例えば上限＝5とした設定をするなど、発行処理における制限を付帯することで、極端な不正利用の発生を防止することが可能である。

上述の審査代行グループ属性証明書の発行処理態様は、Aさんの所有機器をグループとして設定したグループ属性証明書においても同様に処理可能であり、審査代行実行ACを適用した審査代行グループ属性証明書としてAさんが審査代行者として審査代行実行ACに基づいて審査代行グループ属性証明書をAさんの所有機器各々に発行することが可能となる。

さらに、審査代行グループ属性証明書を適用した処理例として、選挙における投票に適用する例がある。審査代行グループ属性証明書を利用することで、有権者が、投票する候補者以外、選挙管理委員にすら誰に投票したかわからないようにして選挙を行うことができる。

この処理例では、

審査代行者：有権者

AC利用者（属性所持者）：候補者

とする。この選挙システムは、投票時に有権者は選挙管理委員と通信する代わりに候補者と通信すればよいというモデルであり、現実の選挙とは異なる。まず、サービスプロバイダ（SP）は、有権者に審査代行実行ACを発行する。有権者は、投票予定の候補者から、ユニークな識別値、すなわち他の投票とかぶらない識別値を教えてもらい、その数と投票予定の候補者のPKCシリアルNo.を属性として持つ審査代行グループ属性証明書（Gp.AC）を審査代行実行ACに基づいて、発行して候補者に送付する。審査代行実行ACは、この審査代行グループ属性証明書（Gp.AC）の生成後、自動的に破棄される。

各候補者に対して発行された審査代行グループ属性証明書（Gp.AC）数に基づいて、得票数がカウントされ、当落を決定する。同じ識別値の書かれた審査代行グループ属性証明書は、コピーしたとみなされ一票にしかならない。

（７－３－２）代理署名実行属性証明書

次に、代理署名実行属性証明書について説明する。代理署名実行ＡＣはＡＣ利用者（属性保持者）自身が、自らサービスに適用するためのグループ属性証明書（代理署名グループ属性証明書）を発行することを可能とした実行属性証明書である。

図８６を参照して代理署名実行属性証明書の概要を説明する。図８６（ａ）は、通常の属性証明書の発行、適用処理形態を示す。属性証明書（ＡＣ）の利用者である属性保持者から例えば属性認証局（ＡＡ）、属性証明書登録局（ＡＲＡ）あるいはサービスプロバイダ（ＳＰ）等の発行者に対して属性証明書、ここではグループ属性証明書（Ｇｐ．ＡＣ）の発行要求（Ｓ９０１）を行なう。例えばこの場合、ＡＣ利用者の属性を証明するデータの提出が必要となる。前述した実施例では、例えばクレジットカード会社がすでにＡＣ利用者に対して発行済みのグループ属性証明書の提示をする例を説明した。

発行者は、ＡＣ利用者の属性等のユーザ確認としての審査を実行（Ｓ９０２）して、審査成立と判定すると、ＡＣ利用者の属性を証明する属性証明書（ここではＧｐ．ＡＣ）９２１を利用者に発行（Ｓ９０３）する。

ＡＣ利用者（属性保持者）は、発行されたグループ属性証明書（Ｇｐ．ＡＣ）をサービスプロバイダ（ＳＰ）等の検証者に提示してサービスの適用を受けることが可能であり、検証者からのグループ属性証明書（Ｇｐ．ＡＣ）提示要求（Ｓ９０４）に応じて、ＡＣ利用者（属性保持者）が提示（Ｓ９０５）を行ない、検証者がグループ属性証明書（Ｇｐ．ＡＣ）の検証（Ｓ９０６）を実行する。

（ｂ）に示す例は、以下において詳細に説明する代理署名実行属性証明書を適用したグループ属性証明書（Ｇｐ．ＡＣ）発行、適用処理シーケンスである。

まず、ＡＣ利用者（属性保持者）は、例えば属性認証局（ＡＡ）、属性証明書登録局（ＡＲＡ）あるいはサービスプロバイダ（ＳＰ）等の発行者に対して代理署名実行属性証明書（ＡＣ）の発行要求（Ｓ９１１）を行なう。発行者は、ＡＣ利用者の属性を証明するデータ、例えば発行済みのグループ属性証明書等

に基づいて審査（Ｓ９１２）を実行し、審査成立と判定すると、代理署名実行属性証明書９２３を発行する。発行者は、この際、代理署名鍵証明書９２４も併せてＡＣ利用者（属性保持者）に提供する。

代理署名鍵証明書９２４は、代理署名生成、検証の際に用いる公開鍵（Ｋｐａ）と、発行者署名データを有する。また、代理署名実行属性証明書９２３は、前述の実行証明書と同様、審査代行者のユーザデバイスの共通鍵メモリの登録鍵（Ｋｃｒ）の格納領域を示すブロックアドレス（Ａｄ）、登録鍵（Ｋｃｒ）で暗号化された実行命令（Ｅｃ（代理署名命令||属性情報||Ｋｓａ;Ｋｃｒ））、発行者署名からなる。

実行命令に含まれる秘密鍵（Ｋｓａ）は、代理署名生成、検証の際に用いる秘密鍵であり、前述の公開鍵（Ｋｐａ）に対応する秘密鍵である。

ステップＳ９１１～Ｓ９１３は、発行フェーズであり、この発行フェーズの完了の後、検証フェーズが開始される。ステップＳ９１４において、サービスプロバイダ（ＳＰ）等の検証者は、ＡＣ利用者（属性保持者）に対して代理署名グループ属性証明書（Ｇｐ．ＡＣ）の提示要求を実行する。この提示要求に際して、サービスプロバイダ（ＳＰ）等の検証者は、代理署名グループ属性証明書（Ｇｐ．ＡＣ）の検証用乱数（Ｒａ）をＡＣ利用者（属性保持者）に対して送信する。

ＡＣ利用者（属性保持者）は、ステップＳ９１５において、サービスプロバイダ（ＳＰ）等の検証者からの代理署名グループ属性証明書（Ｇｐ．ＡＣ）の提示要求に応じて、先に発行者から受領した代理署名実行属性証明書を適用して代理署名グループ属性証明書（Ｇｐ．ＡＣ）９２２を生成する。この生成処理の詳細については後述する。代理署名グループ属性証明書（Ｇｐ．ＡＣ）９２２は、ＡＣ利用者（属性保持者）の公開鍵証明書（ＰＫＣ）のシリアル番号、属性情報等の情報に、検証者から受信した検証用乱数（Ｒａ）を含み、先に、発行者から受領した代理署名実行属性証明書９２３の実行命令中に格納された秘密鍵（Ｋｓａ）を適用した署名が付加される。

ＡＣ利用者（属性保持者）は、生成した代理署名グループ属性証明書９２２と、代理署名鍵証明書９２４を併せて検証者に送付（Ｓ９１６）する。検証者

は、代理署名鍵証明書９２４の署名検証の後、代理署名鍵証明書９２４に格納された代理署名検証用の公開鍵（Ｋｐａ）を取り出して、取り出した公開鍵（Ｋｐａ）を適用して、代理署名グループ属性証明書９２２の署名検証を実行する。さらに、代理署名グループ属性証明書中に格納された乱数と自己が先に生成した乱数の一致を検証することにより、今回の検証で、検証者の要求に対して提示された代理署名グループ属性証明書であることを確認できる。

サービス提供も含めた各エンティテイ間でのデータの流れを図８７を参照して説明する。まず、発行フェーズにおいて、発行者９３１からＡＣ利用者（属性保持者）９３２に対して代理署名鍵証明書９４１、および代理署名実行属性証明書９４２がＡＣ利用者（属性保持者）９３２に送付される。次に、ＡＣ利用者（属性保持者）９３２からサービスプロバイダ（ＳＰ）等の検証者９３３にサービス要求がなされると、検証者９３３は、ＡＣ利用者（属性保持者）９３２に対して代理署名グループ属性証明書（Ｇｐ．ＡＣ）の提示要求を実行する。この提示要求に際して、検証者９３３は、代理署名グループ属性証明書（Ｇｐ．ＡＣ）の検証用乱数（Ｒａ）をＡＣ利用者（属性保持者）９３２に対して送信する。

ＡＣ利用者（属性保持者）９３２は、検証者９３３からの代理署名グループ属性証明書（Ｇｐ．ＡＣ）の提示要求に応じて、先に発行者から受領した代理署名実行属性証明書を適用して代理署名グループ属性証明書（Ｇｐ．ＡＣ）９４３を生成する。代理署名グループ属性証明書（Ｇｐ．ＡＣ）９４３は、ＡＣ利用者（属性保持者）９３２の公開鍵証明書（ＰＫＣ）のシリアル番号、属性情報等の情報に、検証者から受信した検証用乱数（Ｒａ）を含み、先に、発行者から受領した代理署名実行属性証明書９４２の実行命令中に格納された秘密鍵（Ｋｓａ）を適用した署名が付加される。

次に、ＡＣ利用者（属性所有者）９３２は、代理署名グループ属性証明書９４３と、代理署名鍵証明書９４１を検証者に送付し、検証者が、代理署名グループ属性証明書９４３と、代理署名鍵証明書９４１に基づくＡＣ利用者の属性検証を実行し、検証成立を条件としてサービスを提供する。

サービスプロバイダ（ＳＰ）等の検証者９３３は、代理署名鍵証明書９４１

の署名検証の後、代理署名鍵証明書９４１に格納された代理署名検証用の公開鍵（Ｋｐａ）を取り出して、取り出した公開鍵（Ｋｐａ）を適用して代理署名グループ属性証明書９４３の署名検証を実行し、また代理署名グループ属性証明書９４３の格納乱数の照合により検証を行なう。

次に、発行者の発行した代理署名実行属性証明書と代理署名鍵証明書とを有するＡＣ利用者が、サービスプロバイダ（ＳＰ）等の検証者からの代理署名グループ属性証明書の提示要求に際して実行する処理の詳細を図８８を参照して説明する。図８８において、

ＳＰ：属性証明書の検証を実行するサービスプロバイダ制御部、

ＳＭ：ＳＰのセキュリティモジュール

ＥＥ:属性証明書利用ユーザデバイスのエンドエンティテイ（ＥＥ）制御部、

ＳＣ：ＥＥ内に構成されるセキュリティチップ、

実行ＡＣテーブル：ＥＥの実行ＡＣテーブル制御部、

である。

図８８の処理は、サービスプロバイダ（ＳＰ）のセキュリティモジュール（ＳＭ）と、ユーザデバイスのセキュリティチップ（ＳＣ）間で相互認証が成立した後の処理を示している。

相互認証成立の後、サービスプロバイダ（ＳＰ）は、セキュリティモジュール（ＳＭ）に対して、属性証明書検証時に適用する乱数の生成要求（Ｓ９５１）を行なう、ステップＳ９５２において、セキュリティモジュール（ＳＭ）は、要求に応じて乱数を生成しサービスプロバイダ（ＳＰ）に出力する。

ステップＳ９５３において、サービスプロバイダ（ＳＰ）は、エンドエンティテイ（ＥＥ）に対して代理署名グループ属性証明書の提示要求を実行する。この際、サービスプロバイダ（ＳＰ）は、エンドエンティテイ（ＥＥ）に対して代理署名グループ属性証明書（Ｇｐ．ＡＣ）の検証用乱数（Ｒａ）を併せて送信する。

ステップＳ９５４において、エンドエンティテイ（ＥＥ）は、代理署名グループ属性証明書（Ｇｐ．ＡＣ）の生成に適用する代理署名実行属性証明書の検索を実行ＡＣテーブルに対して行ない、実行ＡＣテーブルは、ステップＳ９５

５において、代理署名実行属性証明書およびそれに対応する代理署名鍵証明書をエンドエンティテイ（ＥＥ）に対して出力する。

ステップＳ９５６において、エンドエンティテイ（ＥＥ）は、代理署名実行属性証明書の適用処理、すなわち、代理署名グループ属性証明書の生成処理をセキュリティチップ（ＳＣ）に要求し、ステップＳ９５８において、セキュリティチップ（ＳＣ）は、代理署名グループ属性証明書の生成処理を実行する。この代理署名グループ属性証明書の生成処理の詳細は、先に図８５を参照して説明した審査代行実行属性証明書に基づく審査代行グループ属性証明書の処理と同様である。ただし、代理署名グループ属性証明書には、検証者から受信した乱数（Ｒａ）が格納される。

ステップＳ９５８において、セキュリティチップ（ＳＣ）は、生成した代理署名グループ属性証明書をエンドエンティテイ（ＥＥ）に送付する。エンドエンティテイ（ＥＥ）は、ステップＳ９５９において、代理署名グループ属性証明書、および、先に発行者から受領済みの代理署名鍵証明書をサービスプロバイダ側のセキュリティモジュール（ＳＭ）に送信する。

サービスプロバイダ側のセキュリティモジュール（ＳＭ）が、代理署名グループ属性証明書と、代理署名鍵証明書を受信すると、代理署名鍵証明書に格納された代理署名検証用の公開鍵（Ｋｐａ）を取り出して、取り出した公開鍵（Ｋｐａ）を適用して代理署名グループ属性証明書の署名検証を実行し、また代理署名グループ属性証明書の格納乱数の照合処理に基づく検証を行ない、検証結果をサービスプロバイダ（ＳＰ）に通知する。サービスプロバイダ（ＳＰ）は応答結果に応じて、検証成立の場合はサービス提供を実行し、検証不成立の場合はサービス提供の停止処理を行なうことになる。

代理署名実行属性証明書の適用例として、通常の属性証明書がある。すなわち、通常の属性証明書の代わりに、代理署名実行属性証明書を用いれば、実行属性証明書の破棄処理機能を用いることが出来るので、検証のたびに破棄リストを参照するなどの、失効処理による煩雑さ、信頼性の低下を解決することが出来る。

さらなる適用例としては、属性証明回数を制限した代理署名属性証明書があ

る。すなわち、アクセス許可など、暗号化データの復号以外のサービスに対しても、サービス提供を認めるグループ属性証明書として、回数制限の機能を持った代理署名実行属性証明書を用いれば、サーバ等外部に回数情報を持たせるなどの処理の煩雑さ、処理効率の低下なく、制限されたサービス提供を行うことが出来る。

[（８）各エンティテイの構成]

次に、上述した処理、すなわち属性証明書の生成、検証、送受信等を実行するユーザデバイスとしてのセキュリティチップ（ＳＣ）を備えたエンドエンティテイ（ＥＥ）、あるいはセキュリティチップ（ＳＣ）を備えたユーザ識別デバイス（ＵＩＤ）、あるいはサービスプロバイダ（ＳＰ）等、各エンティテイの情報処理装置としての構成例について図を参照しながら、説明する。

ユーザデバイス、サービスプロバイダ等、各エンティテイの情報処理装置は、各種のデータ処理、および制御を実行するＣＰＵを有し、かつ他エンティテイと通信可能な通信手段を備えた例えば、サーバ、ＰＣ、ＰＤＡ、携帯通信端末装置等の各種の情報処理装置によって構成可能である。

図８９に情報処理装置構成例を示す。なお、図８９に示す構成例は１つの例であり、各エンティテイは、ここに示すべての機能を必ずしも備えることが要求されるものではない。図８９に示すＣＰＵ(Central processing Unit)９５１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実行するプロセッサである。ＲＯＭ（Read-Only-Memory）９５２は、ＣＰＵ９５１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）９５３は、ＣＰＵ９５１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

ＨＤＤ９５４はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。セキュリティチップ９６２は、前述したように耐タンパ構造を持つ構成であり、暗号処理に必要な鍵データ等を格納し、権限確認処理としての属性証明書の検証、ある

いは生成処理等を実行する暗号処理部、データ処理部、メモリを有する。

バス９６０はＰＣＩ（Peripheral Component Interface）バス等により構成され、各モジュール、入出力インタフェース９６１を介した各入出力装置とのデータ転送を可能にしている。

入力部９５５は、例えばキーボード、ポインティングデバイス等によって構成され、ＣＰＵ９５１に各種のコマンド、データを入力するためにユーザにより操作される。出力部９５６は、例えばＣＲＴ、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。

通信部９５７はデバイスの接続したエンティテイ、例えばサービスプロバイダ等との通信処理を実行するネットワークインタフェース、接続機器インタフェース等からなり、ＣＰＵ９５１の制御の下に、各記憶部から供給されたデータ、あるいはＣＰＵ９５１によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティテイからのデータを受信する処理を実行する。

ドライブ９５８は、フレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体９５９の記録再生を実行するドライブであり、各リムーバブル記録媒体９５９からのプログラムまたはデータ再生、リムーバブル記録媒体９５９に対するプログラムまたはデータ格納を実行する。

各記憶媒体に記録されたプログラムまたはデータを読み出してＣＰＵ９５１において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース９６１、バス９６０を介して例えば接続されているＲＡＭ９５３に供給される。

前述の説明内に含まれるユーザデバイス、サービスプロバイダ等における処理を実行するためのプログラムは例えばＲＯＭ９５２に格納されてＣＰＵ９５１によって処理されるか、あるいはハードディスクに格納されＨＤＤ９５４を介してＣＰＵ９５１に供給されて実行される。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかし

ながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

以上、説明したように、本発明の権限管理システム、情報処理装置、および方法によれば、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書をサービス受領エンティテイに発行し、サービス提供時に、提示されるグループ属性証明書の署名検証による改竄有無の検証、グループ属性証明書に格納されたグループ識別情報に基づく、サービス許容グループであるか否かの審査を実行し、審査に基づくサービス提供可否の判定を実行する構成としたので、様々なユーザ集合あるいは機器集合に対応する一括した権限確認が可能となり、個別の権限情報の管理が省略可能となり、効率的な権限管理が可能となる。

さらに、本発明の権限管理システム、情報処理装置、および方法によれば、グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを適用してサービス提供の可否についての判定が可能となり、グループ毎の設定権限の詳細な区別が可能となる。

さらに、本発明の権限管理システム、情報処理装置、および方法によれば、複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を各々実行し、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行することが可能であり、機器に対応して設定されたグループおよびユーザに対して設定されたグループ等の重複条件に基づくサービスの提供等、様々な態様での権限設定が可能となる。

さらに、本発明のアクセス権限管理システム、通信処理装置、および方法によれば、特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに、発行者の電子署名を有するグループ属性証明書に格納されたグループ識別情報に基づいて、アクセス

要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を行い、審査に基づいてアクセス可否の判定を実行する構成としたので、通信処理装置を有するユーザが任意に設定したグループのメンバとしてのユーザまたはユーザ機器としてのアクセス要求元の通信処理装置グループのみにアクセスを許可することが可能となる。

さらに、本発明のアクセス権限管理システム、通信処理装置、および方法によれば、アクセス要求元デバイスを構成する個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、アクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行い、アクセス可否の判定を実行する構成としたので、通信処理装置を変更した場合であっても、個人識別デバイスとしてのユーザ識別デバイスに対して発行したグループ属性証明書に基づく審査においてアクセスを許可することが可能となり、通信処理装置の変更によってアクセスが拒否されてしまうといったことを防止できる。

本発明のデータ処理システム、データ処理装置、および方法によれば、相互に通信可能な複数デバイス間においてデータ処理を実行するデータ処理システムにおいて、通信相手デバイスに対するデータ処理を要求するデータ処理要求元デバイスが、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報としたグループ属性証明書をデータ処理要求先デバイスに対して送信して、データ処理要求先デバイスにおいて、グループ属性証明書の検証処理を実行して、検証に基づいてデータ処理要求元デバイスのデータ処理要求権限の有無を判定し、権限有りの判定に基づいてデータ処理を実行する構成としたので、誤った機器あるいはユーザによる処理が実行されることが防止され、正当な権限に基づく正しいデータ処理が実行されることになる。

さらに、本発明のデータ処理システム、データ処理装置、および方法によれば、複数のデータ処理装置のそれぞれが通信相手デバイスに対して相互にデータ処理を要求し、協業したデータ処理を実行する構成においても、各デバイス各々が、通信相手に対するデータ処理要求時に自デバイスに格納したグループ

属性証明書を送信し、受領デバイスにおける検証成立を条件として、データ処理要求に応じた処理を相互に実行することにより、複数のデータ処理装置における通信を伴う協業したデータ処理を正しく実行することが可能となる。

さらに、本発明のデータ処理システム、データ処理装置、および方法によれば、メンテナンス実行デバイスと、メンテナンスサービス受領デバイスとにそれぞれコントロール属性証明書、サービス属性証明書を格納し、メンテナンスサービス実行時にそれぞれの属性証明書を交換して、各デバイスにおいて相互に検証、審査して、審査成立を条件としたメンテナンス処理を実行する構成としたので、それぞれの設定した権限範囲で、確実なメンテナンス処理を実現することが可能となる。

請求の範囲

1．ユーザデバイスのサービス受領権限を管理する権限管理システムであり、

サービス受領エンティテイとしてのユーザデバイスは、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書を有し、

サービス提供エンティテイとしてのサービスプロバイダは、

前記ユーザデバイスから提示されるグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行する構成を有することを特徴とする権限管理システム。

2．前記グループ属性証明書は、

グループ属性証明書発行エンティテイとユーザデバイス間における相互認証の成立、および、発行対象としての機器またはユーザが前記サービスプロバイダにより許容された発行ポリシーに従っていることを条件として、機器またはユーザに対応するユーザデバイスに対して発行する証明書であることを特徴とする請求項1に記載の権限管理システム。

3．新たなグループ属性証明書の発行処理は、

グループ属性証明書発行エンティテイにおいて、ユーザデバイスが既に有する既発行のグループ属性証明書についての検証成立を条件として行なう構成であることを特徴とする請求項1に記載の権限管理システム。

4．前記サービスプロバイダは、

前記グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを有し、前記ユーザデバイスから提示されるグループ属性証明書に格納されたグループ識別情報に基づいて、前記グループ情報データベースを検索して、サービス提供の可否についての判定処理を実行する構成であることを特徴とする請求項１に記載の権限管理システム。

５．　前記サービスプロバイダは、

前記ユーザデバイスから提示される複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を各々実行し、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行する構成を有することを特徴とする請求項１に記載の権限管理システム。

６．　前記サービスプロバイダは、

前記ユーザデバイスから機器をグループのメンバとしたグループ定義に基づく第１のグループ属性証明書から取得される第１のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行うとともに、ユーザをグループのメンバとしたグループ定義に基づく第２のグループ属性証明書から取得される第２のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行する構成を有することを特徴とする請求項１に記載の権限管理システム。

７．　前記ユーザデバイスは、

前記サービスプロバイダとの通信を実行する機器としてのエンドエンティティ、および個人識別デバイスとしてのユーザ識別デバイスを含み、

前記グループ属性証明書は、前記エンドエンティティおよびユーザ識別デバイス各々に対して個別に発行され、グループ属性証明書発行エンティティと前

記エンドエンティテイ、またはユーザ識別デバイスとの相互認証成立を条件とした発行処理がなされる構成であることを特徴とする請求項１に記載の権限管理システム。

８．　前記グループ属性証明書は、属性認証局の発行する属性証明書であり、属性証明書中の属性情報フィールドに、グループ識別子を格納した構成であることを特徴とする請求項１に記載の権限管理システム。

９．　前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記サービスプロバイダは、

前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行する構成であることを特徴とする請求項１に記載の権限管理システム。

１０．　サービス提供処理としてのデータ処理を実行する情報処理装置であり、

サービス提供先デバイスからサービス利用権限確認処理に適用する属性証明書として、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書を受信するデータ受信部と、

前記グループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行するグループ属性証明書検証処理部と、

を有することを特徴とする情報処理装置。

１１．　前記情報処理装置は、

前記グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを有し、

前記グループ属性証明書検証処理部は、

前記サービス提供先デバイスから提示されるグループ属性証明書に格納されたグループ識別情報に基づいて、前記グループ情報データベースを検索して、サービス提供の可否についての判定処理を実行する構成であることを特徴とする請求項１０に記載の情報処理装置。

１２．　前記グループ属性証明書検証処理部は、

前記ユーザデバイスから提示される複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、該審査に基づくサービス提供可否の判定処理を実行する構成を有することを特徴とする請求項１０に記載の情報処理装置。

１３．　ユーザデバイスのサービス受領権限を管理する権限管理方法であり、

サービス受領エンティテイとしてのユーザデバイスにおける実行ステップとして、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書をサービス提供エンティテイとしてのサービスプロバイダに送信するステップを有し、

前記サービスプロバイダにおける実行ステップとして、

前記ユーザデバイスから提示されるグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行するステップ、

を有することを特徴とする権限管理方法。

１４．　前記権限管理方法において、さらに、

機器またはユーザに対応するユーザデバイスに対して前記グループ属性証

明書を発行するグループ属性証明書発行処理ステップを有し、

該グループ属性証明書発行処理ステップは、

グループ属性証明書発行エンティテイとユーザデバイス間における相互認証の成立、および、発行対象としての機器またはユーザが前記サービスプロバイダにより許容された発行ポリシーに従っていることを条件として、機器またはユーザに対応するユーザデバイスに対してグループ属性証明書を発行する処理ステップであることを特徴とする請求項１３に記載の権限管理方法。

１５．　前記グループ属性証明書発行処理ステップは、

ユーザデバイスが既に有する既発行のグループ属性証明書についての検証処理ステップを含み、該検証の成立を条件としてグループ属性証明書の発行を行なうことを特徴とする請求項１４に記載の権限管理方法。

１６．　前記サービスプロバイダは、

前記グループ識別子と、グループに属するメンバに対する許容サービス情報を対応付けたグループ情報データベースを有し、前記ユーザデバイスから提示されるグループ属性証明書に格納されたグループ識別情報に基づいて、前記グループ情報データベースを検索して、サービス提供の可否についての判定処理を実行することを特徴とする請求項１３に記載の権限管理方法。

１７．　前記サービスプロバイダは、

前記ユーザデバイスから提示される複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を各々実行し、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行することを特徴とする請求項１３に記載の権限管理方法。

１８．　前記サービスプロバイダは、

前記ユーザデバイスから機器をグループのメンバとしたグループ定義に基

づく第１のグループ属性証明書から取得される第１のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行うとともに、ユーザをグループのメンバとしたグループ定義に基づく第２のグループ属性証明書から取得される第２のグループ識別情報に基づいて、サービス許容対象であるか否かの審査を行い、全てのグループ識別情報がサービス許容対象であることの判定を条件としてサービス提供可の判定処理を実行することを特徴とする請求項１３に記載の権限管理方法。

１９．　前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記サービスプロバイダは、

前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行することを特徴とする請求項１３に記載の権限管理方法。

２０．　サービス提供処理としてのデータ処理を実行する情報処理装置における情報処理方法であり、

サービス提供先デバイスからサービス利用権限確認処理に適用する属性証明書として、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書を受信する証明書受信ステップと、

前記グループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行するグループ属性証明書検証処理ステップと、

を有することを特徴とする情報処理方法。

２１．　前記情報処理装置は、

前記グループ識別子と、グループに属するメンバに対する許容サービス情報

を対応付けたグループ情報データベースを有し、

前記グループ属性証明書検証処理ステップは、

前記サービス提供先デバイスから提示されるグループ属性証明書に格納されたグループ識別情報に基づいて、前記グループ情報データベースを検索して、サービス提供の可否についての判定処理を実行するステップを含むことを特徴とする請求項２０に記載の情報処理方法。

２２．　前記グループ属性証明書検証処理ステップは、

前記ユーザデバイスから提示される複数の異なるグループ定義に基づく複数のグループ属性証明書から取得される複数の異なるグループ識別情報に基づいて、サービス許容対象であるか否かの審査を各々実行し、全てのグループ識別情報がサービス許容対象であることの判定を条件として基づくサービス提供可の判定処理を実行するステップを含むことを特徴とする請求項２０に記載の情報処理方法。

２３．　ユーザデバイスのサービス受領権限を管理する権限管理処理を実行せしめるコンピュータ・プログラムであって、

サービス提供先デバイスからサービス利用権限確認処理に適用する属性証明書として、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者の電子署名の付加されたグループ属性証明書を受信するデータ受信ステップと、

前記グループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、サービス許容グループであるか否かの審査を行い、該審査に基づくサービス提供可否の判定を実行するグループ属性証明書検証処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

２４．　通信機能を有する通信機器間におけるアクセス制限を実行するアクセス権限管理システムであり、

アクセス要求元デバイスは、

特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに、発行者の電子署名を有するグループ属性証明書を記憶手段に格納し、

前記アクセス要求元デバイスからのアクセス要求対象となるアクセス要求先デバイスは、

前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とするアクセス権限管理システム。

２５．　前記アクセス要求先デバイスは、

前記アクセス要求元デバイスを構成するアクセス実行機器としてのエンドエンティティに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するエンドエンティティであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とする請求項２４に記載のアクセス権限管理システム。

２６．　前記アクセス要求先デバイスは、

前記アクセス要求元デバイスを構成する個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とする請求項２４に記載のアクセス権限管理システム。

２７．　前記アクセス要求元デバイス、およびアクセス要求先デバイスは、耐タンパ構成を持つセキュリティチップを有し、相互のセキュリティチップ間

における相互認証を実行し、相互認証の成立を条件として、前記アクセス要求先デバイスは、前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証、およびアクセス許容グループに属するデバイスであるか否かの審査を実行する構成であることを特徴とする請求項２４に記載のアクセス権限管理システム。

２８．　前記アクセス要求先デバイスは、

デバイスからのアクセス許容グループメンバであることを証明するグループ属性証明書の発行要求を受領するとともに、

デバイス間の相互認証の成立、および、グループ属性証明書発行要求デバイスが、前記アクセス要求先デバイスの許容する発行ポリシーに従っていることを条件として、機器またはユーザに対応するデバイスに対してアクセス許容グループメンバであることを証明するグループ属性証明書を発行する処理を実行する構成であることを特徴とする請求項２４に記載のアクセス権限管理システム。

２９．　前記アクセス要求先デバイスは、

デバイスからのアクセス許容グループメンバであることを証明するグループ属性証明書の発行要求を受領するとともに、

デバイス間の相互認証の成立、および、グループ属性証明書発行要求デバイスが既に保有する既発行のグループ属性証明書の検証および審査の成立を条件として、アクセス許容グループメンバであることを証明するグループ属性証明書を発行する処理を実行する構成であることを特徴とする請求項２４に記載のアクセス権限管理システム。

３０．　前記グループ属性証明書は、グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記アクセス要求先デバイスは、

前記グループ属性証明書の検証に際し、前記リンク情報によって取得される

公開鍵証明書の検証を併せて実行する構成であることを特徴とする請求項２４に記載のアクセス権限管理システム。

３１．　アクセス制限処理を実行する通信処理装置であり、

アクセス要求元デバイスから特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とし、発行者の電子署名を有するグループ属性証明書を受信する受信部と、

前記アクセス要求元デバイスから受信したグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行するグループ属性証明書検証処理機能を実行するアクセス権限判定処理部と、

を有することを特徴とする通信処理装置。

３２．　前記アクセス権限判定処理部は、

前記アクセス要求元デバイスにおけるアクセス実行機器としてのエンドエンティティに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するエンドエンティティであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とする請求項３１に記載の通信処理装置。

３３．　前記アクセス権限判定処理部は、

前記アクセス要求元デバイスにおける個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行する構成を有することを特徴とする請求項３１に記載の通信処理装置。

３４．　前記通信処理装置は、前記アクセス要求元デバイスとの相互認証を実行する暗号処理部を有し、

前記アクセス権限判定処理部は、

相互認証の成立を条件として、前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証、およびアクセス許容グループに属するデバイスであるか否かの審査を実行する構成を有することを特徴とする請求項３１に記載の通信処理装置。

３５．　前記通信処理装置は、さらに、

特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とし、発行者の電子署名を有するグループ属性証明書を生成する属性証明書生成部を有することを特徴とする請求項３１に記載の通信処理装置。

３６．　前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記アクセス権限判定処理部は、

前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行する構成であることを特徴とする請求項３１に記載の通信処理装置。

３７．　通信機能を有する通信機器間におけるアクセス制限を実行するアクセス権限管理方法であり、

アクセス要求元デバイスにおいて、

特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに、発行者の電子署名を有するグループ属性証明書をアクセス要求対象となるアクセス要求先デバイスに送信するステップと、

前記アクセス要求先デバイスにおいて、

前記アクセス要求元デバイスから提示されるグループ属性証明書を受信するステップと、

該受信グループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を行う審査ステップと、

前記審査ステップの審査結果に基づいてアクセス可否の判定を実行するステップと、

を有することを特徴とするアクセス権限管理方法。

３８．　前記アクセス要求先デバイスは、

前記アクセス要求元デバイスにおけるアクセス実行機器としてのエンドエンティティに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するエンドエンティティであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行することを特徴とする請求項３７に記載のアクセス権限管理方法。

３９．　前記アクセス要求先デバイスは、

前記アクセス要求元デバイスにおける個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行い、該審査に基づいてアクセス可否の判定を実行することを特徴とする請求項３７に記載のアクセス権限管理方法。

４０．　前記アクセス権限管理方法は、さらに、

前記アクセス要求元デバイス、およびアクセス要求先デバイスの有する耐タンパ構成を持つセキュリティチップ間における相互認証実行ステップを有し、

前記アクセス要求先デバイスは、

相互認証の成立を条件として、前記アクセス要求元デバイスから提示される

グループ属性証明書の署名検証、およびアクセス許容グループに属するデバイスであるか否かの審査を実行することを特徴とする請求項３７に記載のアクセス権限管理方法。

４１．　前記アクセス権限管理方法は、さらに、

前記アクセス要求先デバイスにおいて、

デバイスからのアクセス許容グループメンバであることを証明するグループ属性証明書の発行要求を受信するステップと、

デバイス間の相互認証の成立、および、グループ属性証明書発行要求デバイスが、前記アクセス要求先デバイスの許容する発行ポリシーに従っていることを条件として、機器またはユーザに対応するデバイスに対してグループ属性証明書を発行する処理を実行するステップと、

を有することを特徴とする請求項３７に記載のアクセス権限管理方法。

４２．　前記アクセス権限管理方法は、さらに、

前記アクセス要求先デバイスにおける実行ステップとして、

デバイスからのアクセス許容グループメンバであることを証明するグループ属性証明書の発行要求に応じて、デバイス間の相互認証の成立、および、グループ属性証明書発行要求デバイスが既に保有する既発行のグループ属性証明書の検証および審査の成立を条件として、アクセス許容グループメンバであることを証明するグループ属性証明書を発行する処理を実行するステップを含むことを特徴とする請求項３７に記載のアクセス権限管理方法。

４３．　前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記アクセス要求先デバイスは、

前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行することを特徴とする請求項３７に記載のアクセス権限管理方法。

４４．アクセス制限処理を実行する通信処理装置における通信管理方法であり、

アクセス要求元デバイスから特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とし、発行者の電子署名を有するグループ属性証明書を受信する受信ステップと、

前記アクセス要求元デバイスから受信したグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を実行するアクセス権限判定処理ステップと、

該アクセス権限判定処理結果に基づいてアクセス可否の決定を実行するアクセス可否決定処理ステップと、

を有することを特徴とする通信管理方法。

４５．前記アクセス権限判定処理ステップは、

前記アクセス要求元デバイスにおけるアクセス実行機器としてのエンドエンティティに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するエンドエンティティであるか否かの審査を行なうステップを含むことを特徴とする請求項４４に記載の通信管理方法。

４６．前記アクセス権限判定処理ステップは、

前記アクセス要求元デバイスにおける個人識別デバイスとしてのユーザ識別デバイスに対して発行されたグループ属性証明書に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するユーザの所有デバイスであるか否かの審査を行なうステップを含むことを特徴とする請求項４４に記載の通信管理方法。

４７．　前記通信管理方法において、さらに、

前記アクセス要求元デバイスとの相互認証を実行する認証処理ステップを有し、

前記アクセス権限判定処理ステップは、

相互認証の成立を条件として、前記アクセス要求元デバイスから提示されるグループ属性証明書の署名検証、およびアクセス許容グループに属するデバイスであるか否かの審査を実行することを特徴とする請求項４４に記載の通信管理方法。

４８．　前記グループ属性証明書は、該グループ属性証明書に対応する公開鍵証明書に関するリンク情報を格納した構成であり、

前記アクセス権限判定処理ステップは、

前記グループ属性証明書の検証に際し、前記リンク情報によって取得される公開鍵証明書の検証を併せて実行することを特徴とする請求項４４に記載の通信管理方法。

４９．　アクセス制限処理を実行する通信処理装置における通信管理処理を実行せしめるコンピュータ・プログラムであって、

アクセス要求元デバイスから特定通信機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とし、発行者の電子署名を有するグループ属性証明書を受信する受信ステップと、

前記アクセス要求元デバイスから受信したグループ属性証明書の署名検証による改竄有無の検証を実行するとともに、該グループ属性証明書に格納されたグループ識別情報に基づいて、前記アクセス要求元デバイスがアクセス許容グループに属するデバイスであるか否かの審査を実行するアクセス権限判定処理ステップと、

該アクセス権限判定処理結果に基づいてアクセス可否の決定を実行するアクセス可否決定処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

５０．　相互に通信可能な複数デバイス間において、データ通信処理を伴うデータ処理を実行するデータ処理システムであり、

前記複数デバイス中、通信相手デバイスに対するデータ処理を要求するデータ処理要求元デバイスは、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を格納し、データ処理要求処理に際して、該グループ属性証明書をデータ処理要求先デバイスに対して送信し、

前記データ処理要求先デバイスは、

受領したグループ属性証明書の検証処理を実行し、該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定し、権限有りの判定に基づいてデータ処理を実行する構成としたことを特徴とするデータ処理システム。

５１．　データ処理要求元デバイスに格納されるグループ属性証明書は、データ処理要求先デバイスが発行者であり、該データ処理要求先デバイスの電子署名を有し、

前記データ処理要求先デバイスは、

受領したグループ属性証明書の検証処理として、自デバイスの公開鍵を適用した電子署名検証処理を実行する構成であることを特徴とする請求項５０に記載のデータ処理システム。

５２．　前記相互に通信可能な複数デバイスのいずれもが、通信相手デバイスに対するデータ処理を相互に要求するデバイスであり、通信相手デバイスの発行したグループ属性証明書を各々格納した構成を有し、各デバイス各々が、通信相手に対するデータ処理要求時に自デバイスに格納したグループ属性証明書を送信し、受領デバイスにおける検証成立を条件として、データ処理要求に応じた処理を相互に実行する構成であることを特徴とする請求項５０に記

載のデータ処理システム。

５３．　前記相互に通信可能な複数デバイス各々は、耐タンパ構成を持つセキュリティチップを有し、通信相手デバイスに対するデータ処理要求に際して、相互のセキュリティチップ間における相互認証を実行し、相互認証の成立を条件として、デバイス間におけるグループ属性証明書の送信、および送信グループ属性証明書の検証を実行する構成であることを特徴とする請求項５０に記載のデータ処理システム。

５４．　データ処理要求元デバイスに格納されるグループ属性証明書は、データ処理要求先デバイスが発行者であり、

データ処理要求元デバイスとデータ処理要求先デバイス間の相互認証の成立を条件として発行処理がなされることを特徴とする請求項５０に記載のデータ処理システム。

５５．　前記相互に通信可能な複数のデバイス中、少なくとも１以上のデバイスは、

デバイス構成として、他デバイスとの通信処理およびデータ処理を実行するエンドエンティティと、該エンドエンティティとデータ送受信可能な個人識別機能を有するユーザ識別デバイスとを有し、

前記グループ属性証明書が特定のユーザグループの構成メンバに対して発行される場合、前記ユーザ識別デバイスと、グループ属性証明書発行処理実行デバイス間の相互認証の成立を条件とした発行処理がなされる構成であることを特徴とする請求項５０に記載のデータ処理システム。

５６．　前記相互に通信可能な複数デバイスの一方は、デバイスに対するメンテナンス処理を実行するメンテナンス実行デバイスであり、

他方のデバイスは、前記メンテナンス実行デバイスによるメンテナンスサービスを受領するサービス受領デバイスであり、

前記サービス受領デバイスは、前記メンテナンス実行デバイスの発行したグループ属性証明書としてのサービス属性証明書を格納し、

前記メンテナンス実行デバイスは、前記サービス受領デバイスの発行したグループ属性証明書としてのコントロール属性証明書を格納し、

前記サービス属性証明書は、前記サービス受領デバイスがメンテナンスサービス受領権限を有する機器またはユーザのグループに属することを前記メンテナンス実行デバイスにおいて検証するために適用され、

前記コントロール属性証明書は、前記メンテナンス実行デバイスが、メンテナンスサービス実行権限を有する機器またはユーザのグループに属することを前記サービス受領デバイスにおいて検証するために適用される構成であることを特徴とする請求項５０に記載のデータ処理システム。

５７．　前記サービス受領デバイスにおいて実行されるメンテナンスプログラムは、

暗号化メンテナンスプログラムとして、前記サービス受領デバイスに送信または格納され、

前記サービス受領デバイスは、前記暗号化メンテナンスプログラムを耐タンパ構成を有するセキュリティチップ内で復号した後、前記サービス受領デバイスにおいて実行する構成であることを特徴とする請求項５６に記載のデータ処理システム。

５８．　前記サービス受領デバイスにおいて実行されるメンテナンス処理は、前記メンテナンス実行デバイスから前記サービス受領デバイスに対して送信されるコマンドに基づいて実行され、

前記サービス受領デバイスは、受信コマンドの実行結果を前記メンテナンス実行デバイスに応答送信し、前記メンテナンス実行デバイスは、該応答送信に基づく新たなコマンド送信を前記サービス受領デバイスに対して実行する構成であることを特徴とする請求項５６に記載のデータ処理システム。

５９．　データ処理要求デバイスからのデータ処理要求に基づくデータ処理を実行するデータ処理装置であり、

前記データ処理要求デバイスから、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を受信するデータ受信部と、

受領したグループ属性証明書の検証処理を実行し、該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定する権限判定処理部と、

権限有りの判定に基づいてデータ処理を実行するデータ処理部と、

を有することを特徴とするデータ処理装置。

６０．　前記権限判定処理部は、

受領したグループ属性証明書の検証処理として、自デバイスの公開鍵を適用した電子署名検証処理を実行する構成であることを特徴とする請求項５９に記載のデータ処理装置。

６１．　前記データ処理装置は、

耐タンパ構成を持ち暗号処理部を有するセキュリティチップを有し、

前記暗号処理部は、

データ処理要求デバイスからのデータ処理要求に応じて、データ処理要求デバイスとの相互認証を実行する構成を有し、

前記権限判定処理部は、

相互認証の成立を条件として、グループ属性証明書の検証を実行する構成であることを特徴とする請求項５９に記載のデータ処理装置。

６２．　前記データ処理装置は、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに電子署名を有するグループ属性証明書を生成する機能を持つ属性証明書生成処理部を有する構成であること

を特徴とする請求項５９に記載のデータ処理装置。

６３．　相互に通信可能な複数デバイス間において、データ通信処理を伴うデータ処理を実行するデータ処理方法であり、

前記複数デバイス中、通信相手デバイスに対するデータ処理を要求するデータ処理要求元デバイスにおいて、

特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を、データ処理要求処理に際して、該グループ属性証明書をデータ処理要求先デバイスに対して送信するステップを実行し、

前記データ処理要求先デバイスは、

受領したグループ属性証明書の検証処理ステップ、

該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定するステップ、

権限有りの判定に基づいてデータ処理を実行するステップ、

を実行することを特徴とするデータ処理方法。

６４．　データ処理要求元デバイスに格納されるグループ属性証明書は、データ処理要求先デバイスが発行者であり、該データ処理要求先デバイスの電子署名を有し、

前記データ処理要求先デバイスにおける前記検証処理ステップは、

受領したグループ属性証明書の検証処理として、自デバイスの公開鍵を適用した電子署名検証処理を実行することを特徴とする請求項６３に記載のデータ処理方法。

６５．　前記相互に通信可能な複数デバイスのいずれもが、通信相手デバイスに対するデータ処理を相互に要求するデバイスであって、通信相手デバイスの発行したグループ属性証明書を各々格納した構成を有し、各デバイスいずれもが、通信相手に対するデータ処理要求時に自デバイスに格納したグループ属

性証明書を送信し、受領デバイスにおける検証成立を条件として、データ処理要求に応じた処理を相互に実行することを特徴とする請求項６３に記載のデータ処理方法。

６６．　前記相互に通信可能な複数デバイス各々は、耐タンパ構成を持つセキュリティチップを有し、通信相手デバイスに対するデータ処理要求に際して、相互のセキュリティチップ間における相互認証を実行し、相互認証の成立を条件として、デバイス間におけるグループ属性証明書の送信、および送信グループ属性証明書の検証を実行することを特徴とする請求項６３に記載のデータ処理方法。

６７．　前記データ処理方法において、さらに、

データ処理要求元デバイスに格納されるグループ属性証明書の発行処理ステップを有し、該発行処理ステップは、

データ処理要求元デバイスとデータ処理要求先デバイス間の相互認証の成立を条件として実行することを特徴とする請求項６３に記載のデータ処理方法。

６８．　前記データ処理方法において、さらに、

データ処理要求元デバイスに格納されるグループ属性証明書の発行処理ステップを有し、該発行処理ステップは、

前記グループ属性証明書を特定のユーザグループの構成メンバに対して発行する場合、データ処理要求元デバイスを構成する個人識別機能を有するユーザ識別デバイスとの相互認証の成立を条件とした発行処理を行なうことを特徴とする請求項６３に記載のデータ処理方法。

６９．　前記相互に通信可能な複数デバイスの一方は、デバイスに対するメンテナンス処理を実行するメンテナンス実行デバイスであり、他方のデバイスは、前記メンテナンス実行デバイスによるメンテナンスサービスを受領するサ

ービス受領デバイスであり、

前記サービス受領デバイスにおける、前記メンテナンス実行デバイスの発行したグループ属性証明書としてのサービス属性証明書を前記メンテナンス実行デバイスに送信するステップと、

前記メンテナンス実行デバイスにおける、受信サービス属性証明書の検証を実行するサービス属性証明書検証ステップと、

前記メンテナンス実行デバイスにおける、前記サービス受領デバイスの発行したグループ属性証明書としてのコントロール属性証明書を前記サービス受領デバイスに送信するステップと、

前記サービス受領デバイスにおける、受信コントロール属性証明書の検証を実行するコントロール属性証明書検証ステップと、

前記サービス属性証明書検証、およびコントロール属性証明書検証の両検証が成立したことを条件としてメンテナンス処理を実行するメンテナンス処理ステップと、

を有することを特徴とする請求項６３に記載のデータ処理方法。

７０．　前記サービス受領デバイスにおいて実行されるメンテナンス処理プログラムは、

暗号化メンテナンスプログラムとして、前記サービス受領デバイスに送信または格納され、

前記サービス受領デバイスは、前記暗号化メンテナンスプログラムを耐タンパ構成を有するセキュリティチップ内で復号した後、前記サービス受領デバイスにおいて実行することを特徴とする請求項６９に記載のデータ処理方法。

７１．　前記サービス受領デバイスにおいて実行されるメンテナンス処理は、前記メンテナンス実行デバイスから前記サービス受領デバイスに対して送信されるコマンドに基づいて実行され、

前記サービス受領デバイスは、受信コマンドの実行結果を前記メンテナンス実行デバイスに応答送信し、前記メンテナンス実行デバイスは、該応答送信に

基づく新たなコマンド送信を前記サービス受領デバイスに対して実行することを特徴とする請求項６９に記載のデータ処理方法。

７２．　データ処理要求デバイスからのデータ処理要求に基づくデータ処理を実行するデータ処理方法であり、

前記データ処理要求デバイスから、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を受信するデータ受信ステップと、

受信したグループ属性証明書の検証処理を実行し、該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定する権限判定処理ステップと、

権限有りの判定に基づいてデータ処理を実行するデータ処理ステップと、

を有することを特徴とするデータ処理方法。

７３．　前記権限判定処理ステップは、

受領したグループ属性証明書の検証処理として、自デバイスの公開鍵を適用した電子署名検証処理を実行するステップを含むことを特徴とする請求項７２に記載のデータ処理方法。

７４．　前記データ処理方法において、さらに、

データ処理要求デバイスからのデータ処理要求に応じて、データ処理要求デバイスとの相互認証を実行するステップを有し、

前記権限判定処理ステップは、

相互認証の成立を条件として、グループ属性証明書の検証を実行することを特徴とする請求項７２に記載のデータ処理方法。

７５．　データ処理要求デバイスからのデータ処理要求に基づくデータ処理を実行せしめるコンピュータ・プログラムであって、

前記データ処理要求デバイスから、特定機器または特定ユーザの集合からなるグループに対応して設定されるグループ識別情報を格納情報とするとともに発行者電子署名を有するグループ属性証明書を受信するデータ受信ステップと、

受領したグループ属性証明書の検証処理を実行し、該検証に基づいて前記データ処理要求元デバイスのデータ処理要求権限の有無を判定する権限判定処理ステップと、

権限有りの判定に基づいてデータ処理を実行するデータ処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

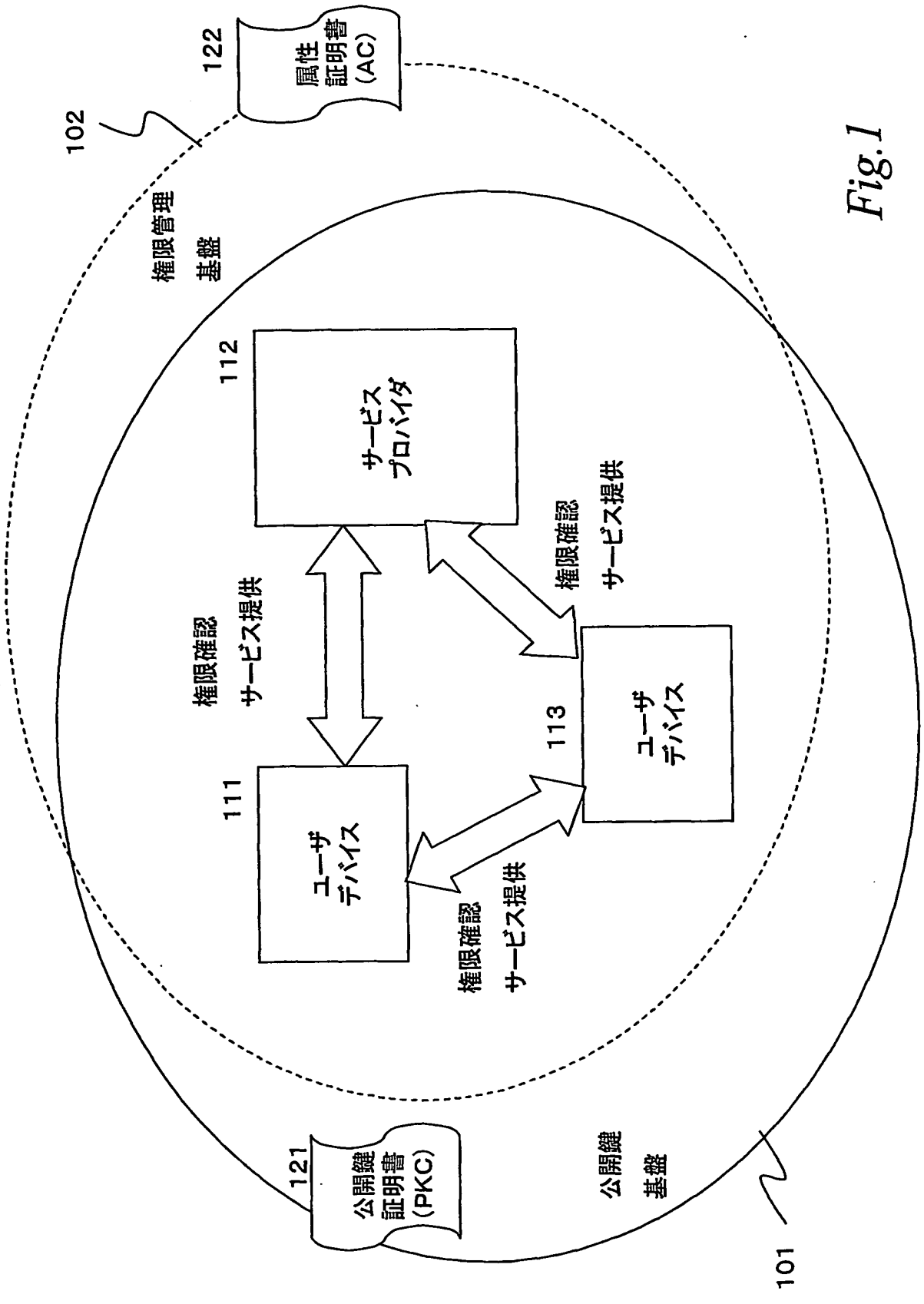
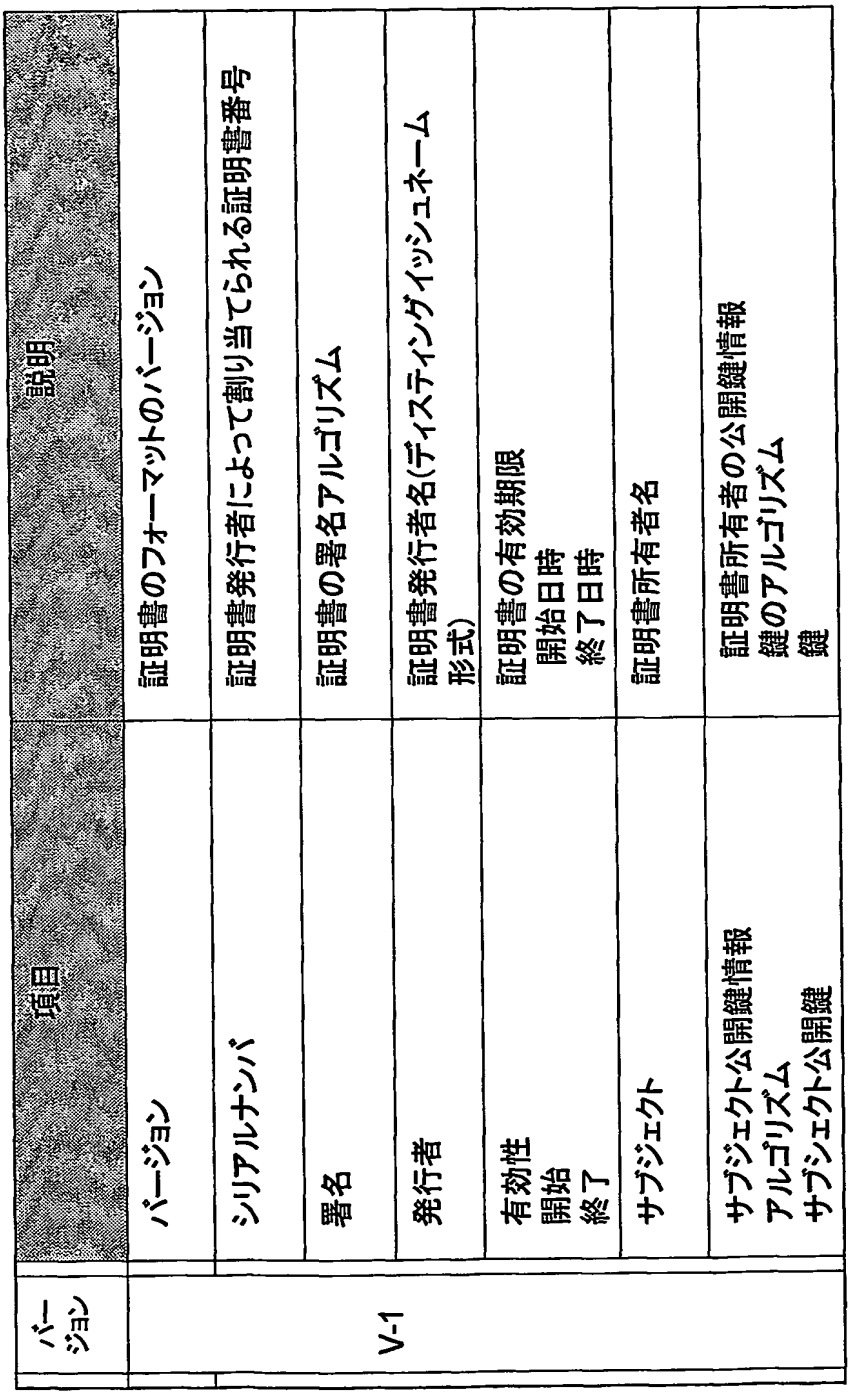

101
公開鍵
基盤
102
権限管理
基盤
121
公開鍵
証明書
(PKC)
122
属性
証明書
(AC)
111
ユーザ
デバイス
112
サービス
プロバイダ
113
ユーザ
デバイス
権限確認
サービス提供
権限確認
サービス提供
権限確認
サービス提供

Fig. 1



バージョン	項目	説明
V-1	バージョン	証明書のフォーマットのバージョン
	シリアルナンバ	証明書発行者によって割り当てられる証明書番号
	署名	証明書の署名アルゴリズム
	発行者	証明書発行者名(ディスティングイッシュネーム形式)
	有効性 開始 終了	証明書の有効期限 開始日時 終了日時
	サブジェクト	証明書所有者名
	サブジェクト公開鍵情報 アルゴリズム サブジェクト公開鍵	証明書所有者の公開鍵情報 鍵のアルゴリズム 鍵

Fig.2

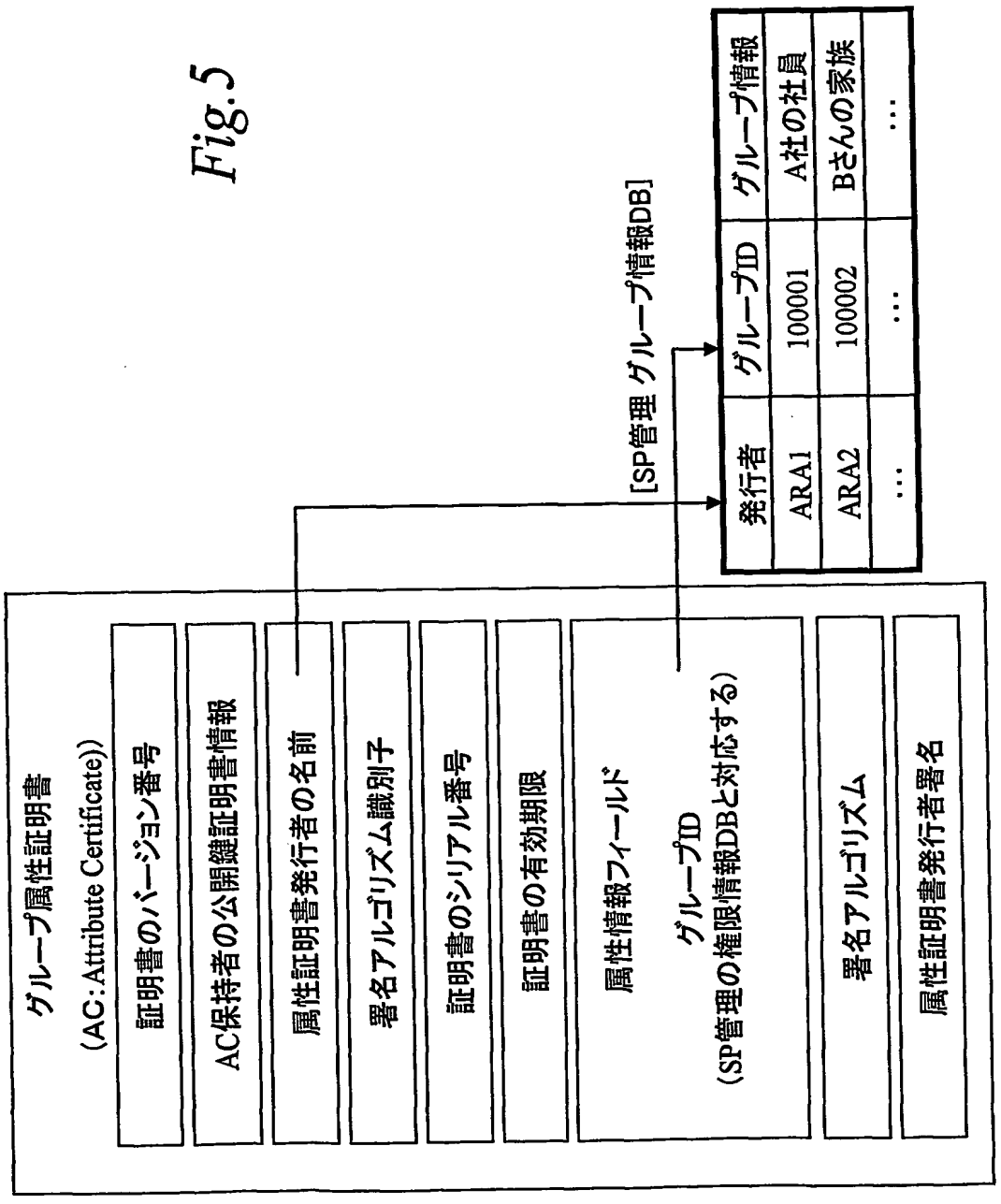
V-3	オーソリティ鍵識別子 鍵識別子 オーソリティ証明書発行者名 オーソリティ証明書シリアルナンバ	署名検証に用いる証明書発行者の鍵識別子 鍵識別子 機関証明書発行者名(General Name形式) 機関証明書シリアルナンバ
	サブジェクト鍵識別子 鍵識別子	複数の鍵の中から目的の鍵を明確に識別
	鍵使用目的 (0)デジタルシグネチャ (1)ノンリピュディエーション (2)キーエンサイファメント (3)データエンサイファメント (4)キーアグリーメント (5)キーサート・サイン (6)cRLサイン	鍵の使用目的を指定 (0)デジタル署名用 (1)否認防止用 (2)鍵の暗号化用 (3)メッセージの暗号化用 (4)共通鍵配送用 (5)認証の署名確認用 (6)失効リストの署名確認用
	秘密鍵有効期限 開始 終了	証明書中の公開鍵に対応する秘密鍵の有効期限
	サーチィフィケートポリシー ポリシー識別子 ポリシークォリファイア	証明書発行者が承認した証明書ポリシー ポリシーID(ISO/IEC9834-1準拠) 認証基準
	ポリシーマッピング 発行者ドメインポリシー サブジェクトドメインポリシー	認証パス中のポリシーの関係を制限 (CA証明書にのみ必要)

Fig.3

V-3	サブジェクト代替ネーム	証明書所有者の別名(GN形式)
	発行者別名	証明書発行者の別名(GN形式)
	サブジェクトディレクトリアトリビュート	証明書所有者のために必要とされるディレクトリの属性
	ベッシークコンストレイント CA パスレンコンストレイント	証明対象の公開鍵が認証局の署名用か、証明書所有者のものかを区別
	ネームコンストレイント パーミットサブツリー ベース ミニマム マキシマム 除外サブツリー	発行者が発行する証明書の名前を制限
	ポリシーコンストレイント リクワイァエクスプリシットポリシー インヒビットポリシーマッピング	認証パス中のポリシーの関係を制限
	CRLディストリビューションポイント	証明書所有者が証明書を利用する際に、証明書が失効していないかどうかを確認するための失効リストの参照点を記述
	シグネチャアルゴリズム	証明書への署名付けに用いるアルゴリズム
	シグネチャバリュー	証明書発行者の秘密鍵による署名

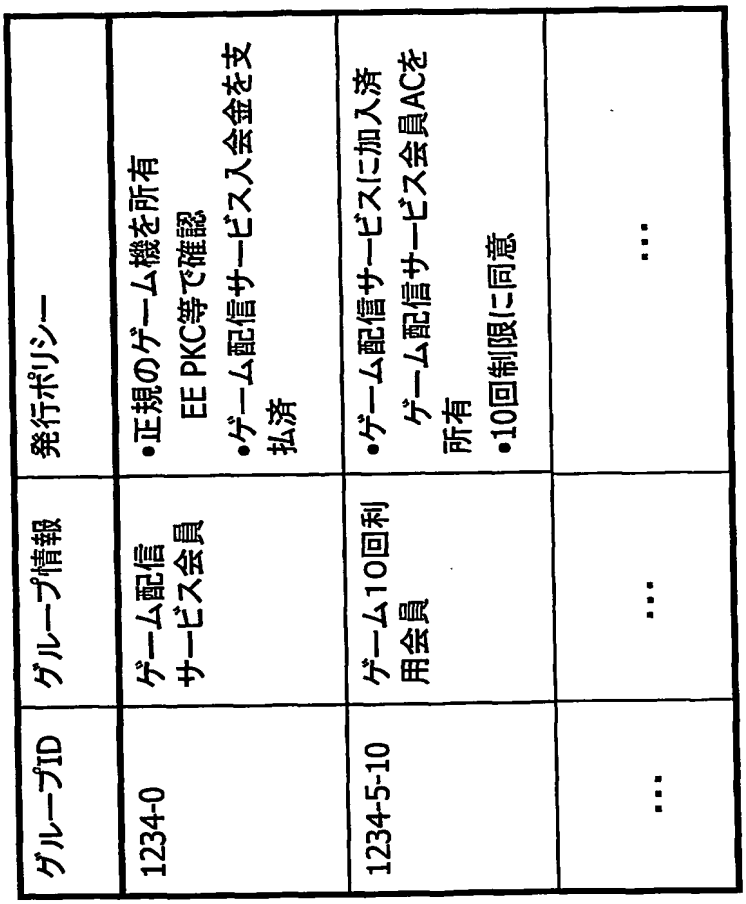
Fig.4

Fig.5


グループ属性証明書
(AC: Attribute Certificate))
証明書のバージョン番号
AC保持者の公開鍵証明書情報
属性証明書発行者の名前
署名アルゴリズム識別子
証明書のシリアル番号
証明書の有効期限
属性情報フィールド
グループID
(SP管理の権限情報DBと対応する)
署名アルゴリズム
属性証明書発行者署名
[SP管理 グループ情報DB]
発行者
グループID
グループ情報
ARA1
100001
A社の社員
ARA2
100002
Bさんの家族
…
…
…

発行者	所有者	検証者	属性情報
グループARA	SC, USC	SP_SM	グループID

Fig.6



グループID	グループ情報	発行ポリシー
1234-0	ゲーム配信サービス会員	•正規のゲーム機を所有 EE PKC等で確認 •ゲーム配信サービス入会金を支払済
1234-5-10	ゲーム10回利用会員	•ゲーム配信サービスに加入済 ゲーム配信サービス会員ACを所有 •10回制限に同意
...	...	...

Fig.7

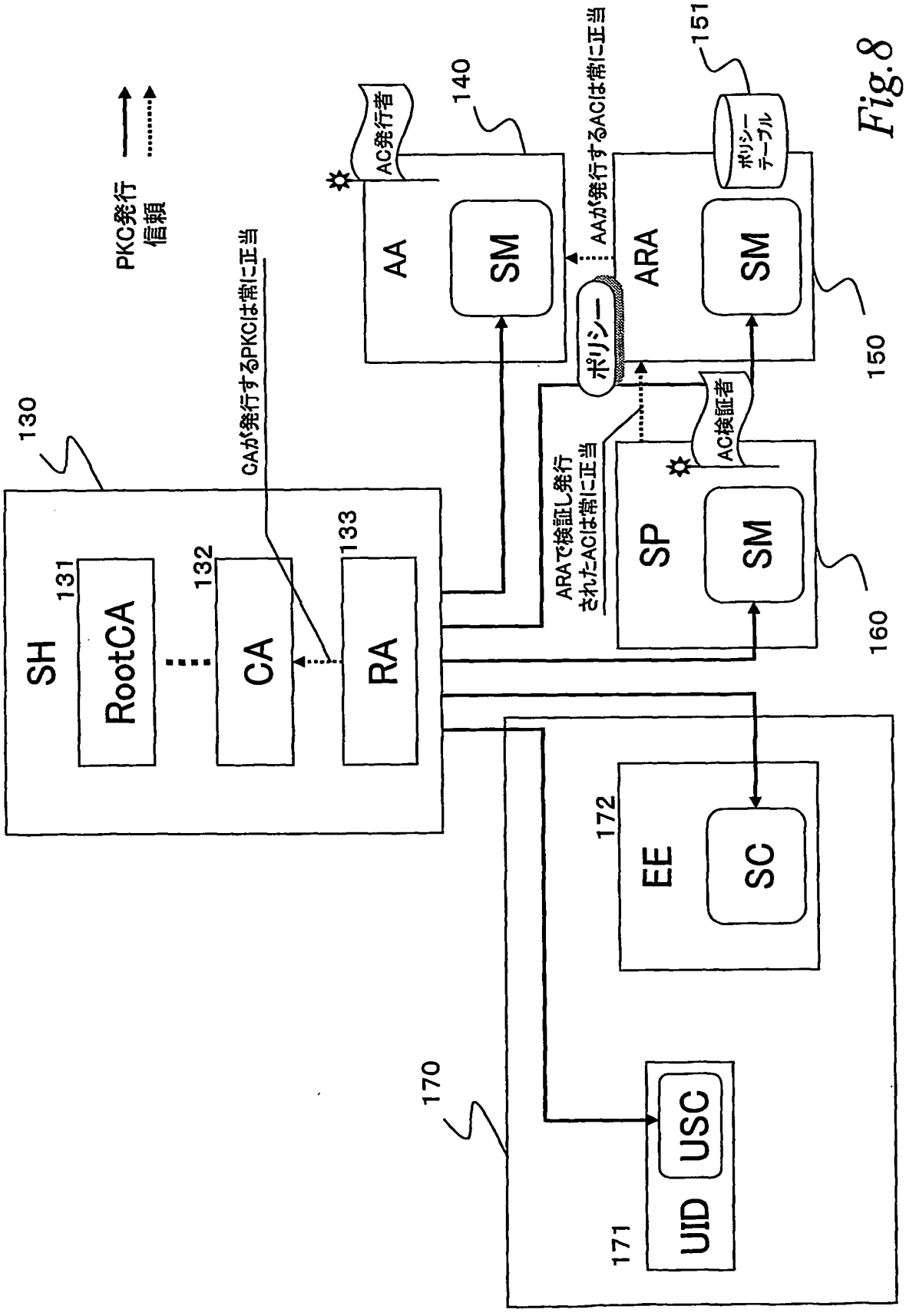

PKC発行
信頼
130
SH
131
RootCA
132
CA
133
RA
CAが発行するPKCは常に正当
140
AC発行者
AA
SM
AAが発行するACは常に正当
ポリシー
151
ポリシーテーブル
ARA
SM
150
ARAで検証し発行されたACは常に正当
AC検証者
SP
SM
160
172
EE
SC
170
171
UID
USC

Fig.8

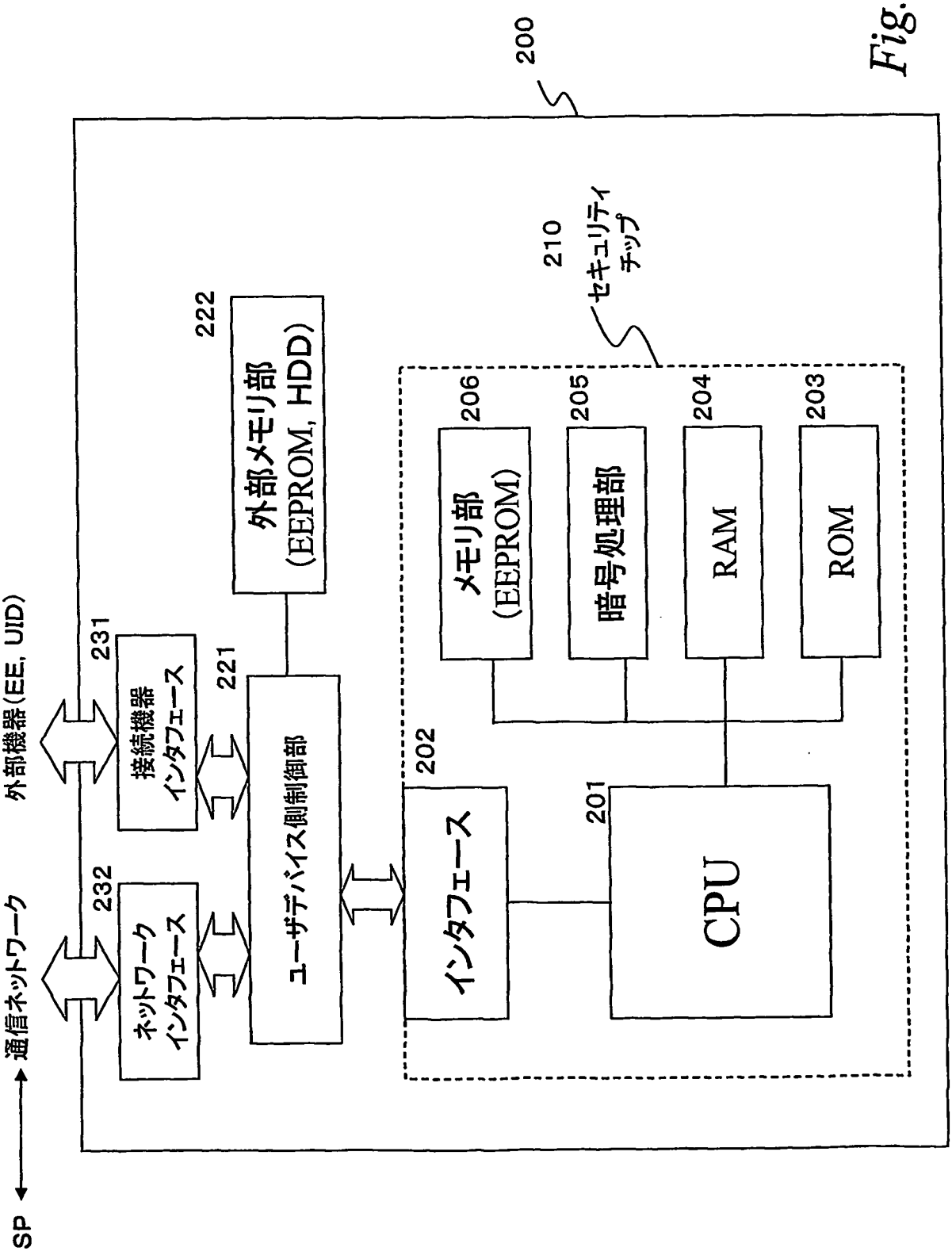

SP
通信ネットワーク
外部機器(EE, UID)
200
210
セキュリティチップ
222
外部メモリ部
(EEPROM, HDD)
231
接続機器
インタフェース
232
ネットワーク
インタフェース
221
ユーザデバイス側制御部
202
インタフェース
201
CPU
206
メモリ部
(EEPROM)
205
暗号処理部
204
RAM
203
ROM

Fig.9

データ種別	データ内容
公開鍵証明書	・ルート認証局公開鍵証明書 ・サービスプロバイダ公開鍵証明書
グループ属性証明書	・機器の属するまたはユーザの属する グループ対応の属性証明書
実行属性証明書	・暗号化実行命令、暗号化実行命令の復号用 登録鍵を格納したメモリのアドレスデータを 含む属性証明書
鍵データ	・セキュリティチップ公開鍵、秘密鍵ペア ・登録鍵 ・リセット鍵 ・乱数生成用鍵、・相互認証用鍵
識別情報	・セキュリティチップID ・サービスプロバイダID ・ユーザID ・アプリケーションID
その他	・乱数シード(Seed) ・サービス利用情報等

Fig.10

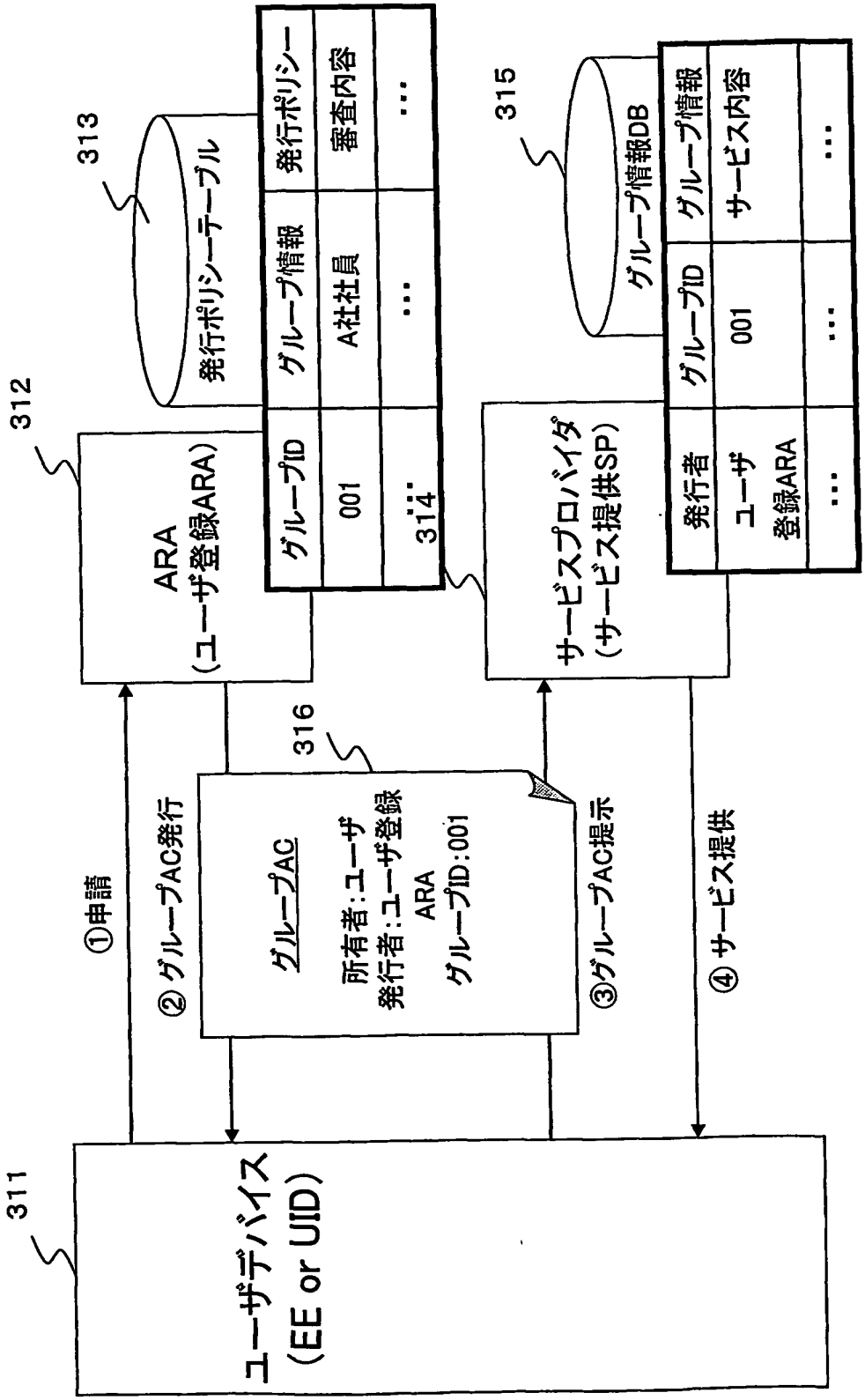

311
ユーザデバイス
(EE or UID)
312
ARA
(ユーザ登録ARA)
313
発行ポリシーテーブル
グループID
001
314
グループ情報
A社社員
発行ポリシー
審査内容
315
サービスプロバイダ
(サービス提供SP)
グループ情報DB
発行者
ユーザ
登録ARA
グループID
001
グループ情報
サービス内容
316
グループAC
所有者:ユーザ
発行者:ユーザ登録
ARA
グループID:001
①申請
②グループAC発行
③グループAC提示
④サービス提供

Fig.11

Fig.12

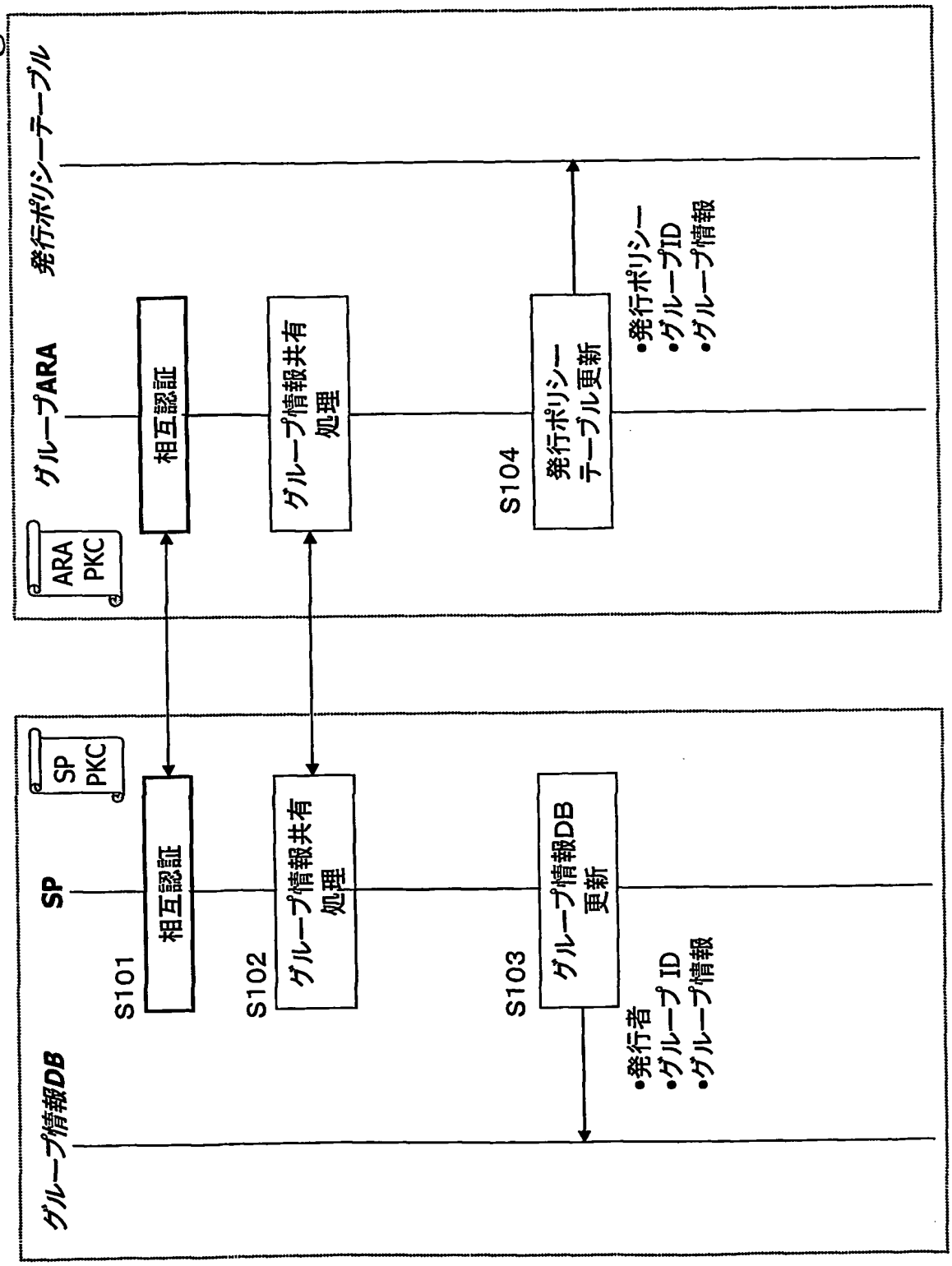
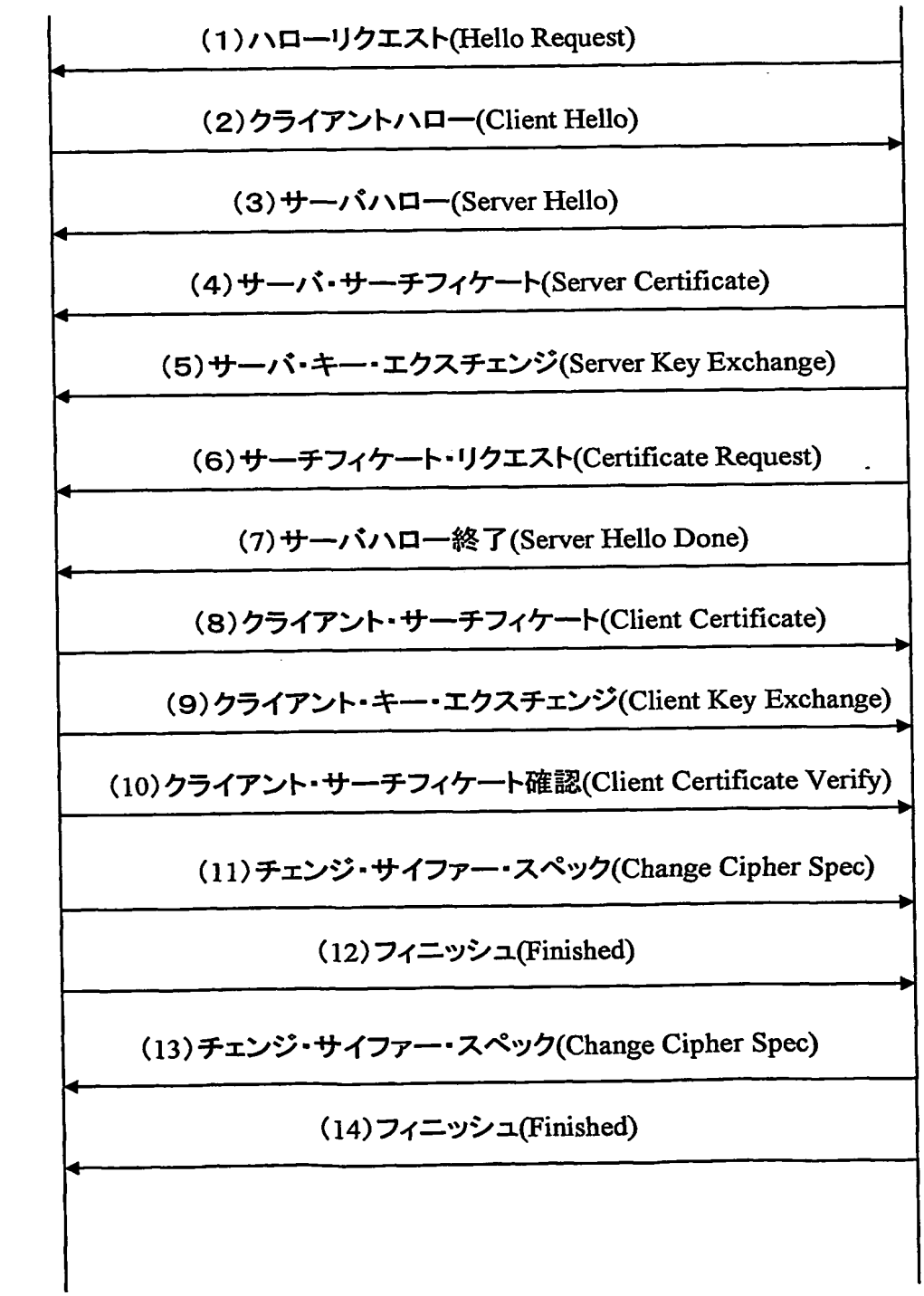

グループ情報DB
SP
SP PKC
S101
相互認証
S102
グループ情報共有処理
S103
グループ情報DB更新
•発行者
•グループ ID
•グループ情報
グループARA
発行ポリシーテーブル
ARA PKC
相互認証
グループ情報共有処理
S104
発行ポリシーテーブル更新
•発行ポリシー
•グループID
•グループ情報

Fig.13


エンティティA
(クライアント)
エンティティB
(サーバ)
(1)ハローリクエスト(Hello Request)
(2)クライアントハロー(Client Hello)
(3)サーバハロー(Server Hello)
(4)サーバ・サーチフィケート(Server Certificate)
(5)サーバ・キー・エクスチェンジ(Server Key Exchange)
(6)サーチフィケート・リクエスト(Certificate Request)
(7)サーバハロー終了(Server Hello Done)
(8)クライアント・サーチフィケート(Client Certificate)
(9)クライアント・キー・エクスチェンジ(Client Key Exchange)
(10)クライアント・サーチフィケート確認(Client Certificate Verify)
(11)チェンジ・サイファー・スペック(Change Cipher Spec)
(12)フィニッシュ(Finished)
(13)チェンジ・サイファー・スペック(Change Cipher Spec)
(14)フィニッシュ(Finished)

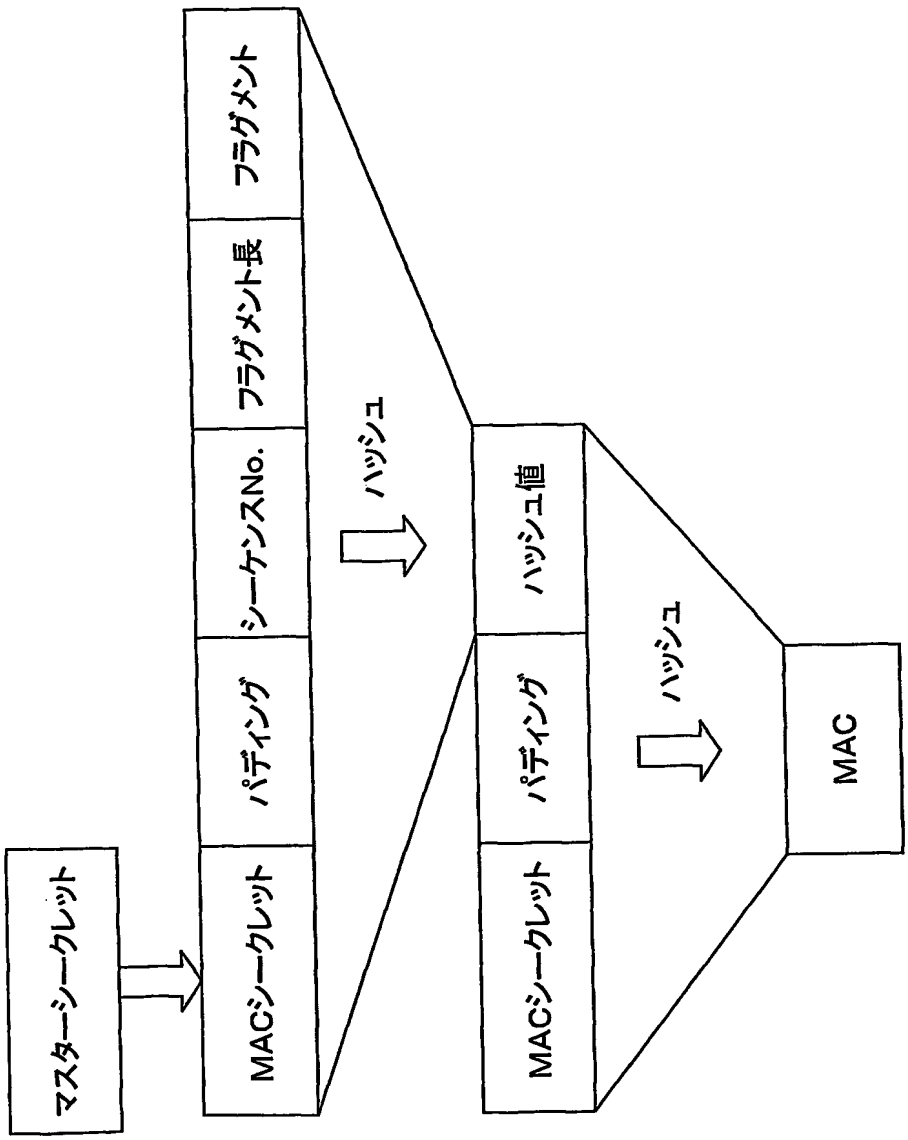

マスターシークレット
MACシークレット
パディング
シーケンスNo.
フラグメント長
フラグメント
ハッシュ
MACシークレット
パディング
ハッシュ値
ハッシュ
MAC

Fig.14

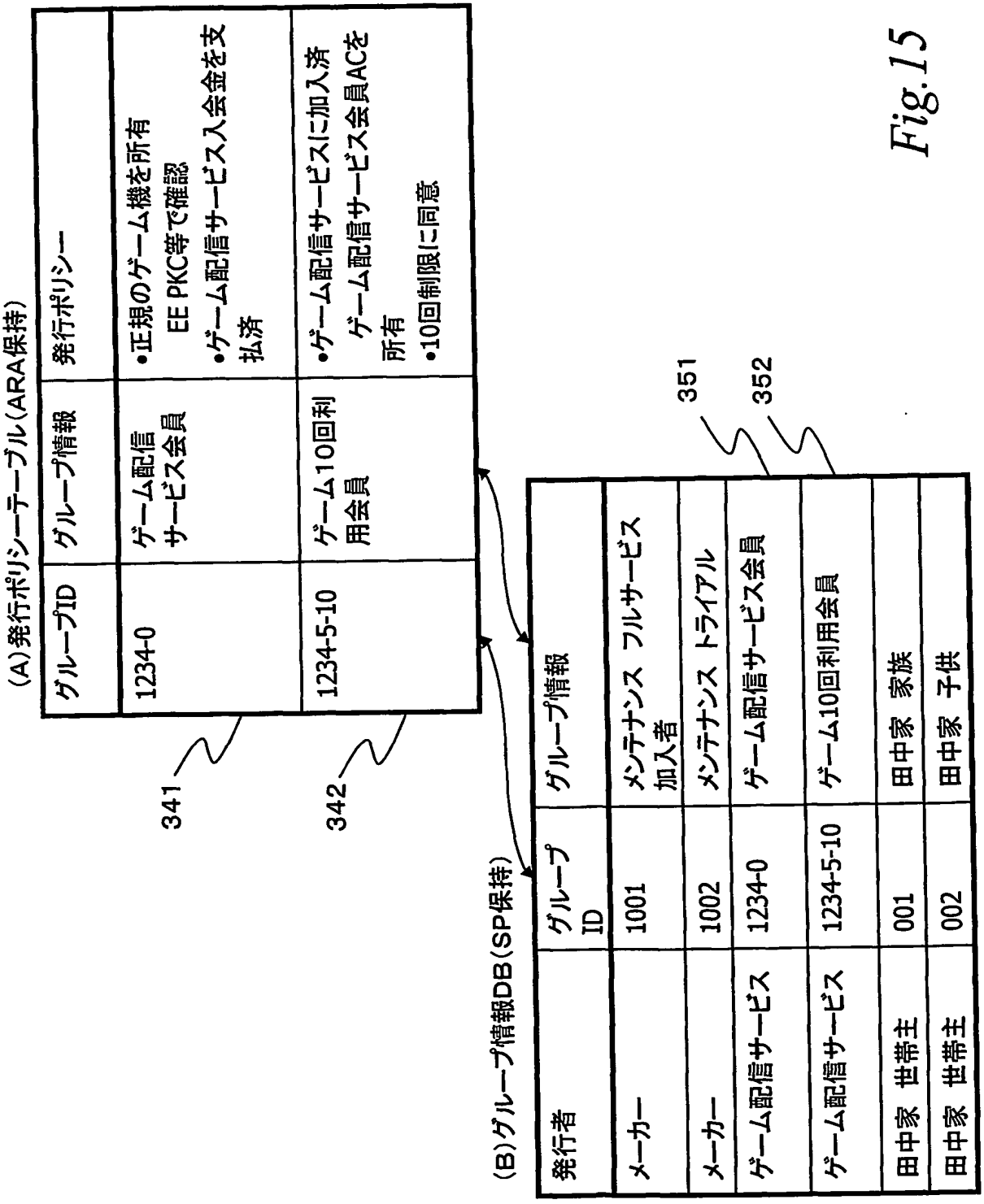

(A)発行ポリシーテーブル(ARA保持)
グループID
グループ情報
発行ポリシー
1234-0
ゲーム配信サービス会員
•正規のゲーム機を所有 EE PKC等で確認
•ゲーム配信サービス入会金を支払済
1234-5-10
ゲーム10回利用会員
•ゲーム配信サービスに加入済 ゲーム配信サービス会員ACを所有
•10回制限に同意
341
342
(B)グループ情報DB(SP保持)
発行者
グループID
グループ情報
メーカー
1001
メンテナンス フルサービス加入者
メーカー
1002
メンテナンス トライアル
ゲーム配信サービス
1234-0
ゲーム配信サービス会員
ゲーム配信サービス
1234-5-10
ゲーム10回利用会員
田中家 世帯主
001
田中家 家族
田中家 世帯主
002
田中家 子供
351
352

Fig.15

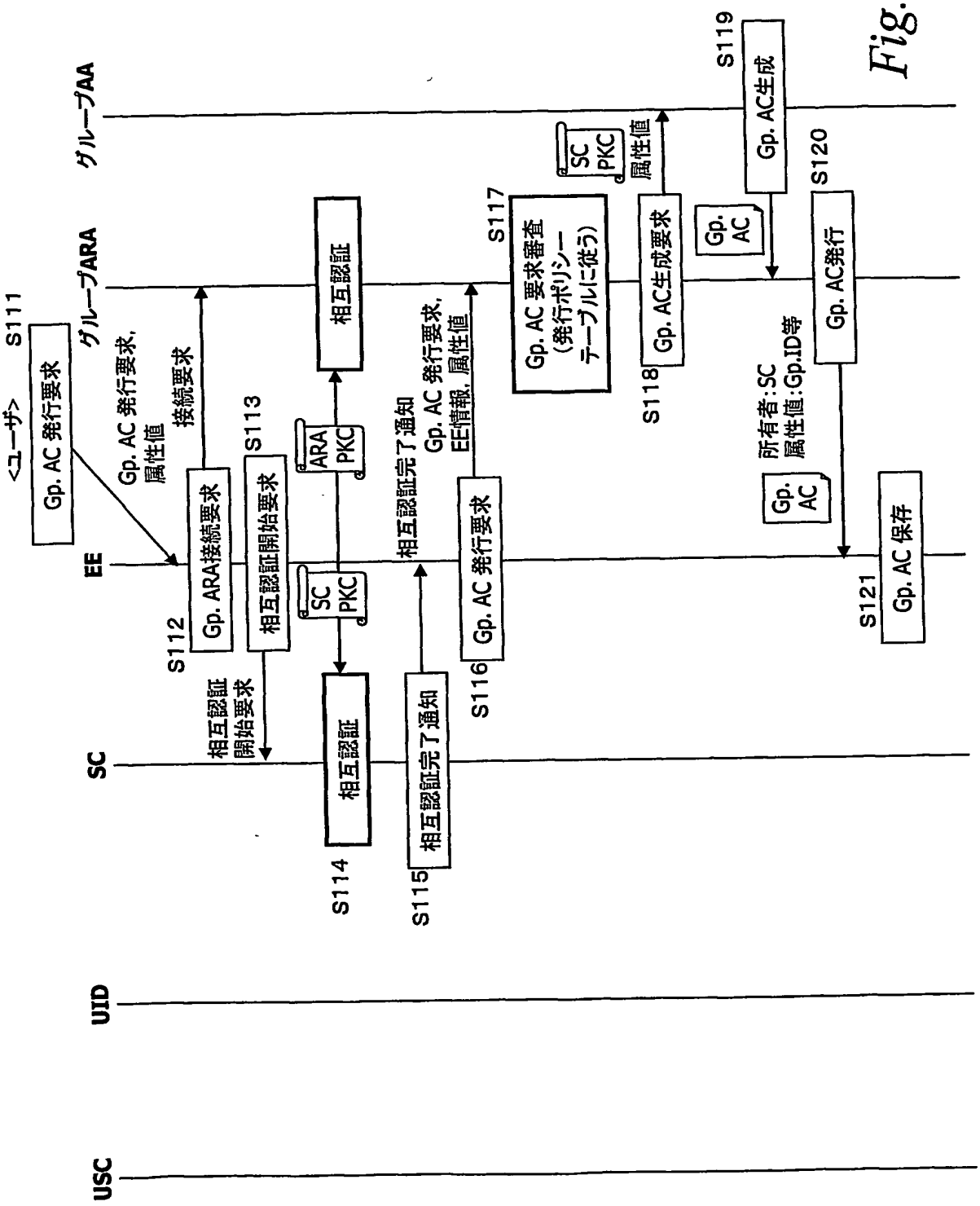

USC
UID
SC
EE
グループARA
グループAA
<ユーザ>
S111
Gp. AC 発行要求
Gp. AC 発行要求,
属性値
接続要求
S112
Gp. ARA接続要求
S113
相互認証開始要求
ARA
PKC
SC
PKC
相互認証
相互認証開始要求
S114
相互認証
S115
相互認証完了通知
相互認証完了通知
Gp. AC 発行要求,
EE情報, 属性値
S116
Gp. AC 発行要求
S117
Gp. AC 要求審査
(発行ポリシー
テーブルに従う)
SC
PKC
属性値
S118
Gp. AC生成要求
S119
Gp. AC生成
Gp.
AC
S120
Gp. AC発行
所有者:SC
属性値:Gp.ID等
Gp.
AC
S121
Gp. AC 保存

Fig.16

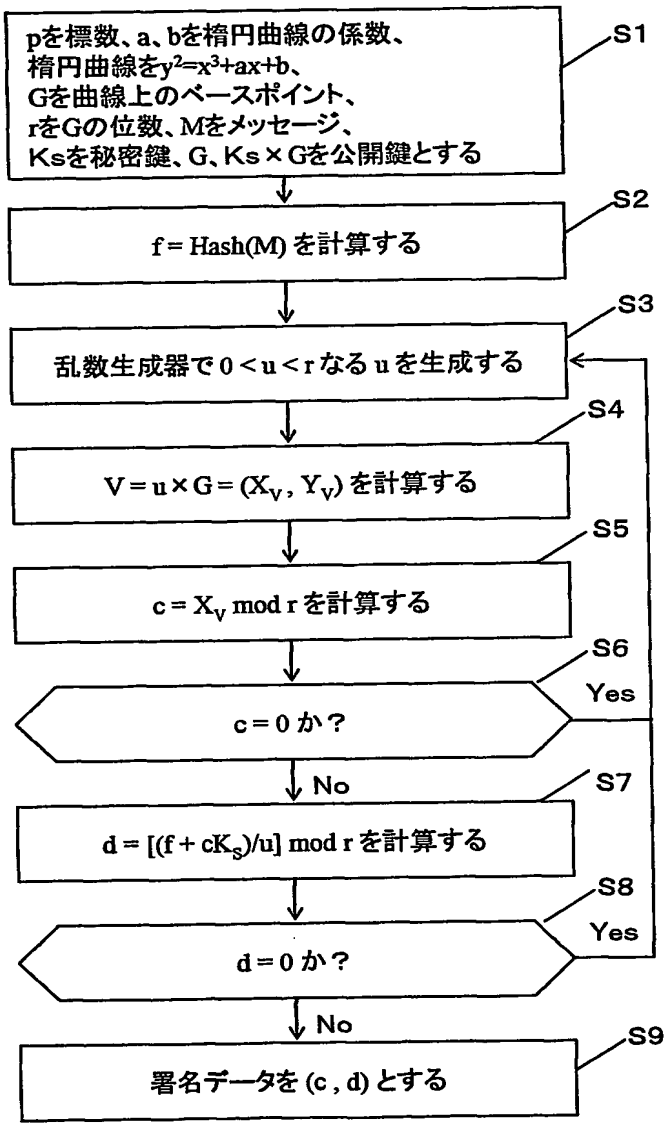

pを標数、a、bを楕円曲線の係数、
楕円曲線を$y^2=x^3+ax+b$、
Gを曲線上のベースポイント、
rをGの位数、Mをメッセージ、
Ksを秘密鍵、G、Ks×Gを公開鍵とする
S1
f = Hash(M) を計算する
S2
乱数生成器で 0 < u < r なる u を生成する
S3
$V = u \times G = (X_V, Y_V)$ を計算する
S4
$c = X_V \bmod r$ を計算する
S5
c = 0 か？
S6
Yes
No
$d = [(f + cK_S)/u] \bmod r$ を計算する
S7
d = 0 か？
S8
Yes
No
署名データを (c , d) とする
S9

Fig.17

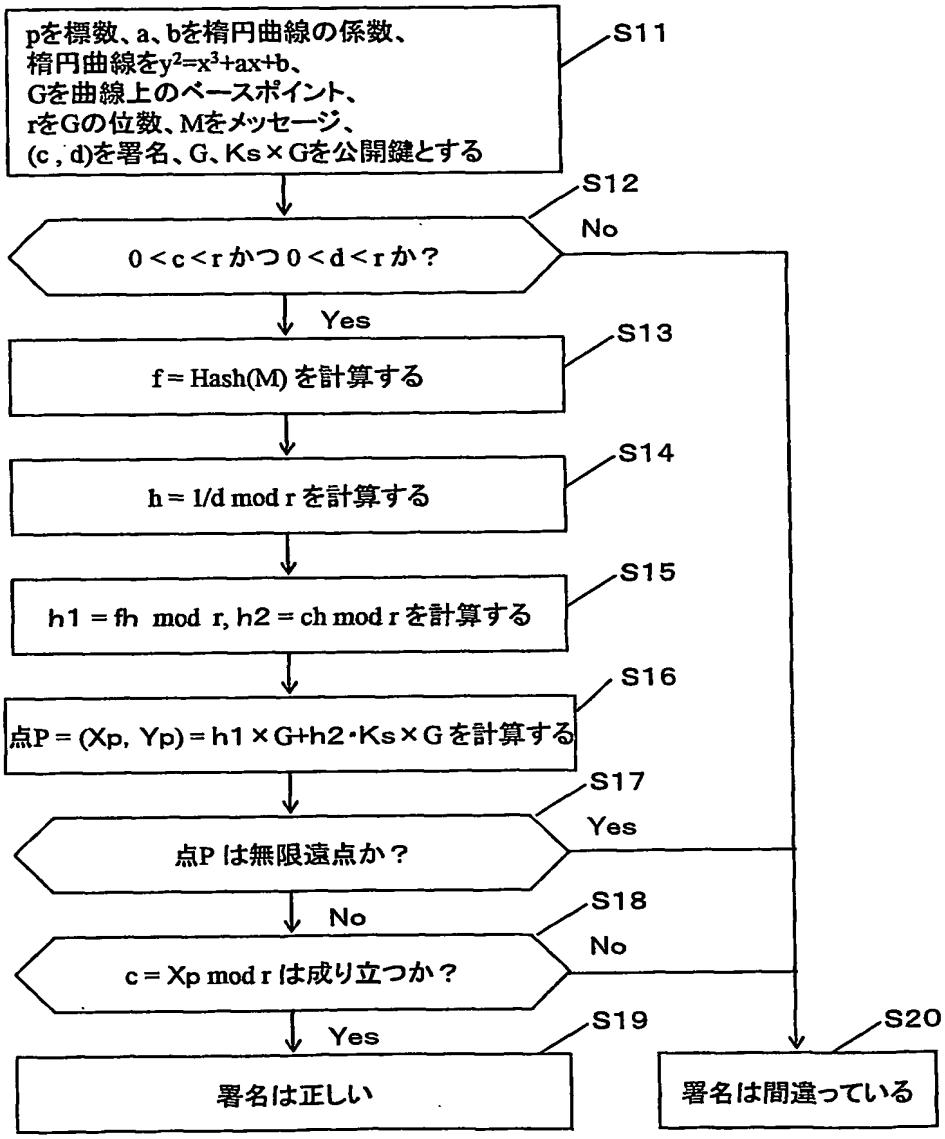

pを標数、a、bを楕円曲線の係数、
楕円曲線を$y^2=x^3+ax+b$、
Gを曲線上のベースポイント、
rをGの位数、Mをメッセージ、
(c , d)を署名、G、Ks×Gを公開鍵とする
S11
S12
0＜c＜rかつ0＜d＜rか？
No
Yes
S13
f = Hash(M) を計算する
S14
h = 1/d mod r を計算する
S15
h1 = fh mod r, h2 = ch mod r を計算する
S16
点P = (Xp, Yp) = h1×G+h2・Ks×G を計算する
S17
点P は無限遠点か？
Yes
No
S18
c = Xp mod r は成り立つか？
No
Yes
S19
署名は正しい
S20
署名は間違っている

Fig.18

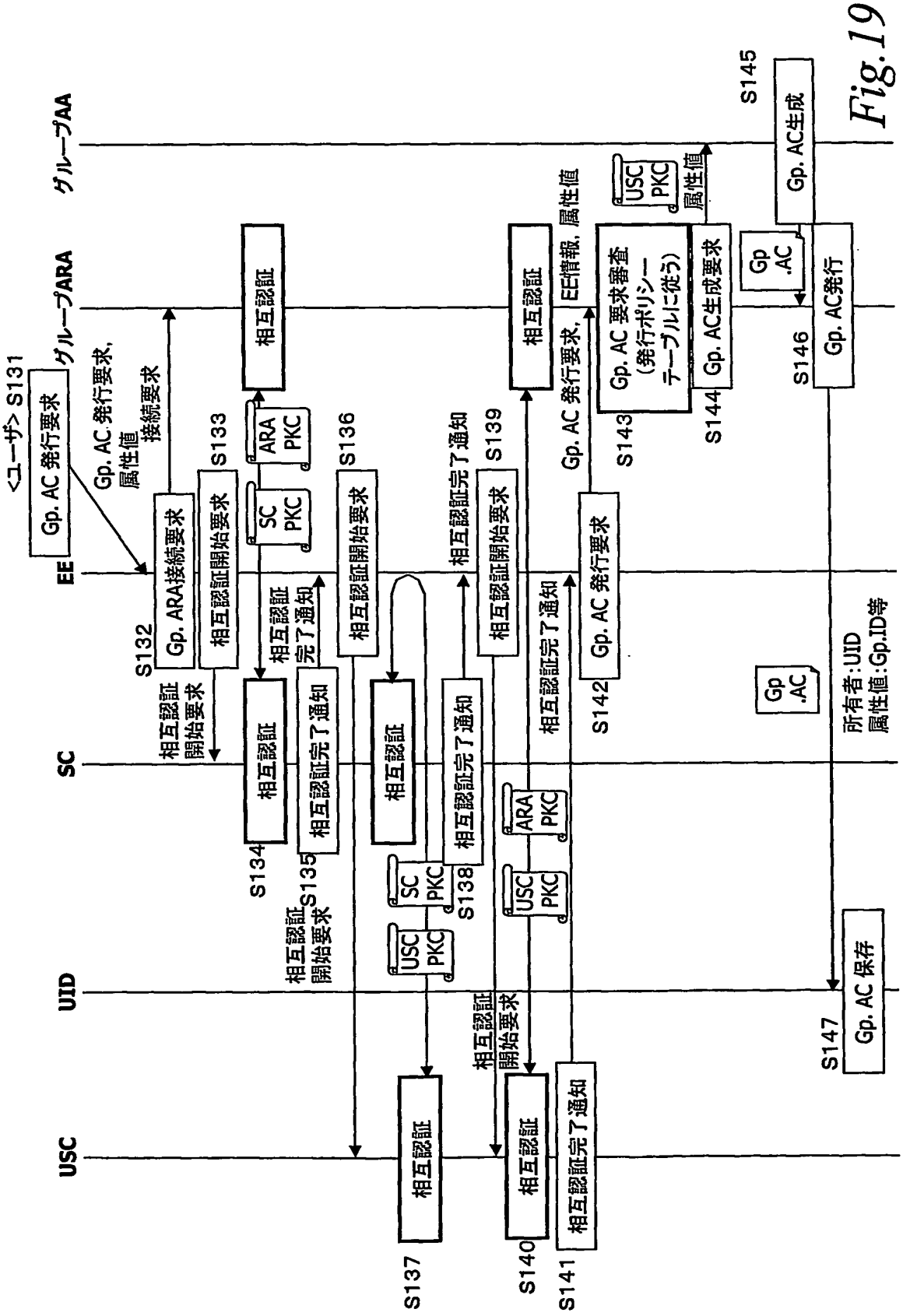

<ユーザ> S131
Gp. AC 発行要求
Gp. AC 発行要求, 属性値 接続要求
Gp. ARA接続要求
S132
相互認証開始要求
S133
相互認証
ARA PKC
SC PKC
相互認証完了通知
S134
相互認証
S135
相互認証開始要求
相互認証
S136
相互認証開始要求
USC PKC
SC PKC
S138
相互認証完了通知
相互認証開始要求
S139
相互認証
ARA PKC
USC PKC
相互認証完了通知
Gp. AC 発行要求
S142
Gp. AC 発行要求
EE情報, 属性値
Gp. AC 要求審査 (発行ポリシーテーブルに従う)
S143
USC PKC 属性値
Gp. AC生成要求
S144
Gp. AC生成
S145
Gp .AC
Gp. AC発行
S146
Gp .AC
所有者:UID
属性値:Gp.ID等
Gp. AC 保存
S147
相互認証
S137
相互認証開始要求
相互認証
S140
相互認証完了通知
S141
グループAA
グループARA
EE
SC
UID
USC

Fig. 19

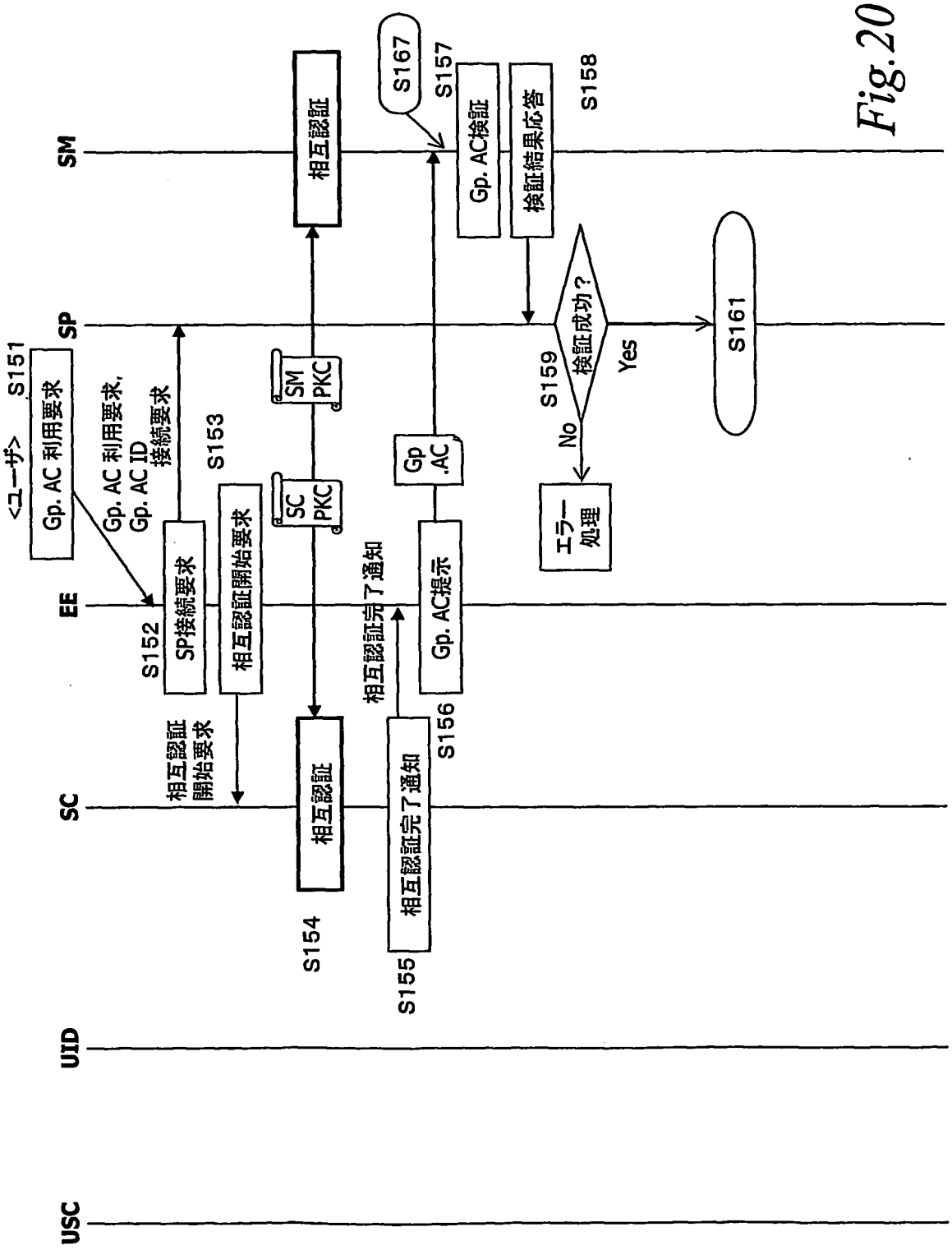

USC
UID
SC
EE
SP
SM
<ユーザ>
Gp. AC 利用要求
S151
Gp. AC 利用要求,
Gp. AC ID
接続要求
S153
SP接続要求
S152
相互認証開始要求
相互認証
開始要求
相互認証
S154
SC
PKC
SM
PKC
相互認証
相互認証完了通知
S155
相互認証完了通知
S156
Gp
.AC
Gp. AC提示
S167
S157
Gp. AC検証
検証結果応答
S158
S159
検証成功?
No
Yes
エラー
処理
S161

Fig. 20

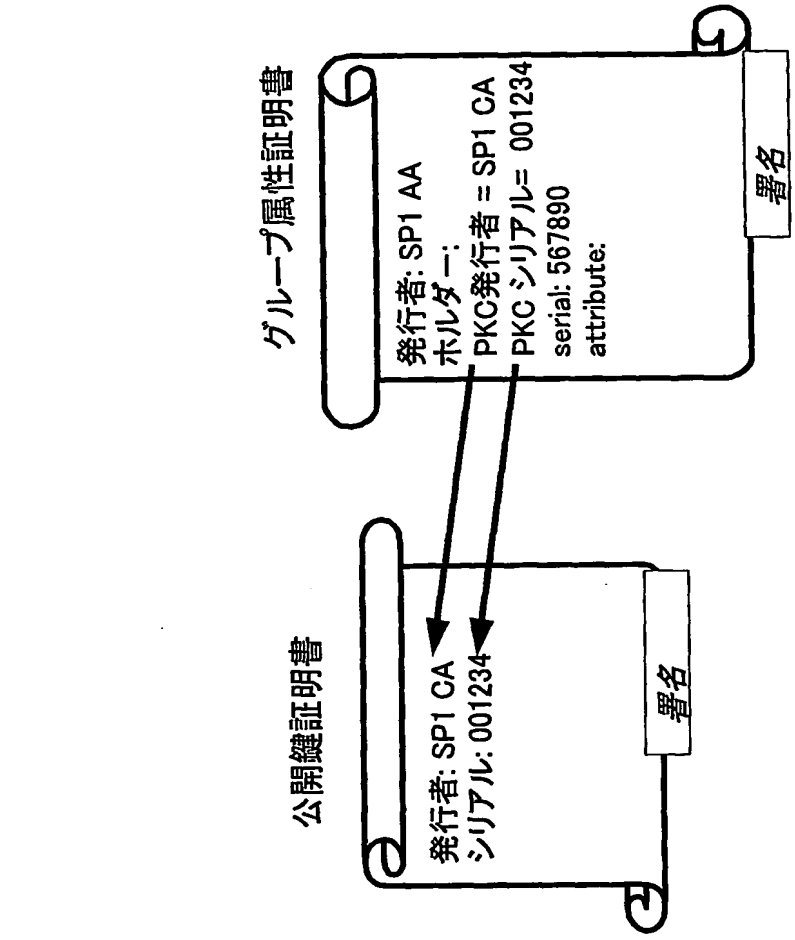
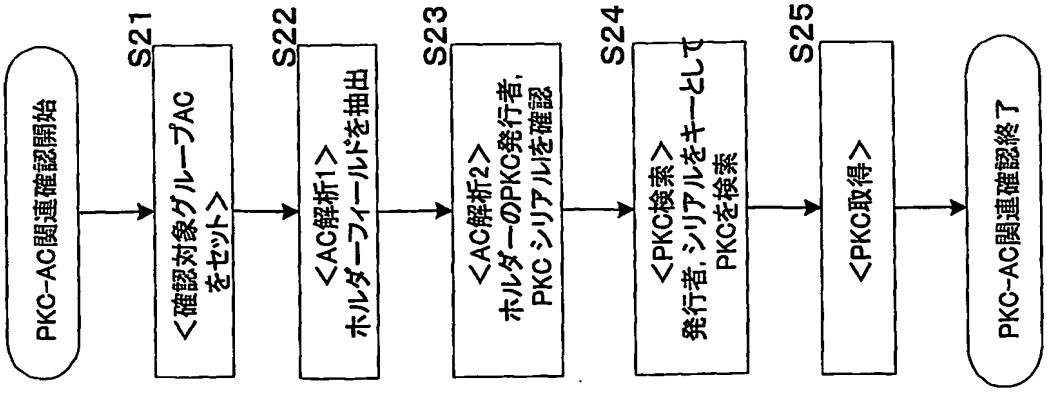

グループ属性証明書
発行者: SP1 AA
ホルダー:
PKC発行者 = SP1 CA
PKC シリアル= 001234
serial: 567890
attribute:
署名
公開鍵証明書
発行者: SP1 CA
シリアル: 001234
署名

Fig.21


PKC-AC関連確認開始
S21
<確認対象グループAC をセット>
S22
<AC解析1> ホルダーフィールドを抽出
S23
<AC解析2> ホルダーのPKC発行者, PKC シリアルを確認
S24
<PKC検索> 発行者, シリアルをキーとして PKCを検索
S25
<PKC取得>
PKC-AC関連確認終了

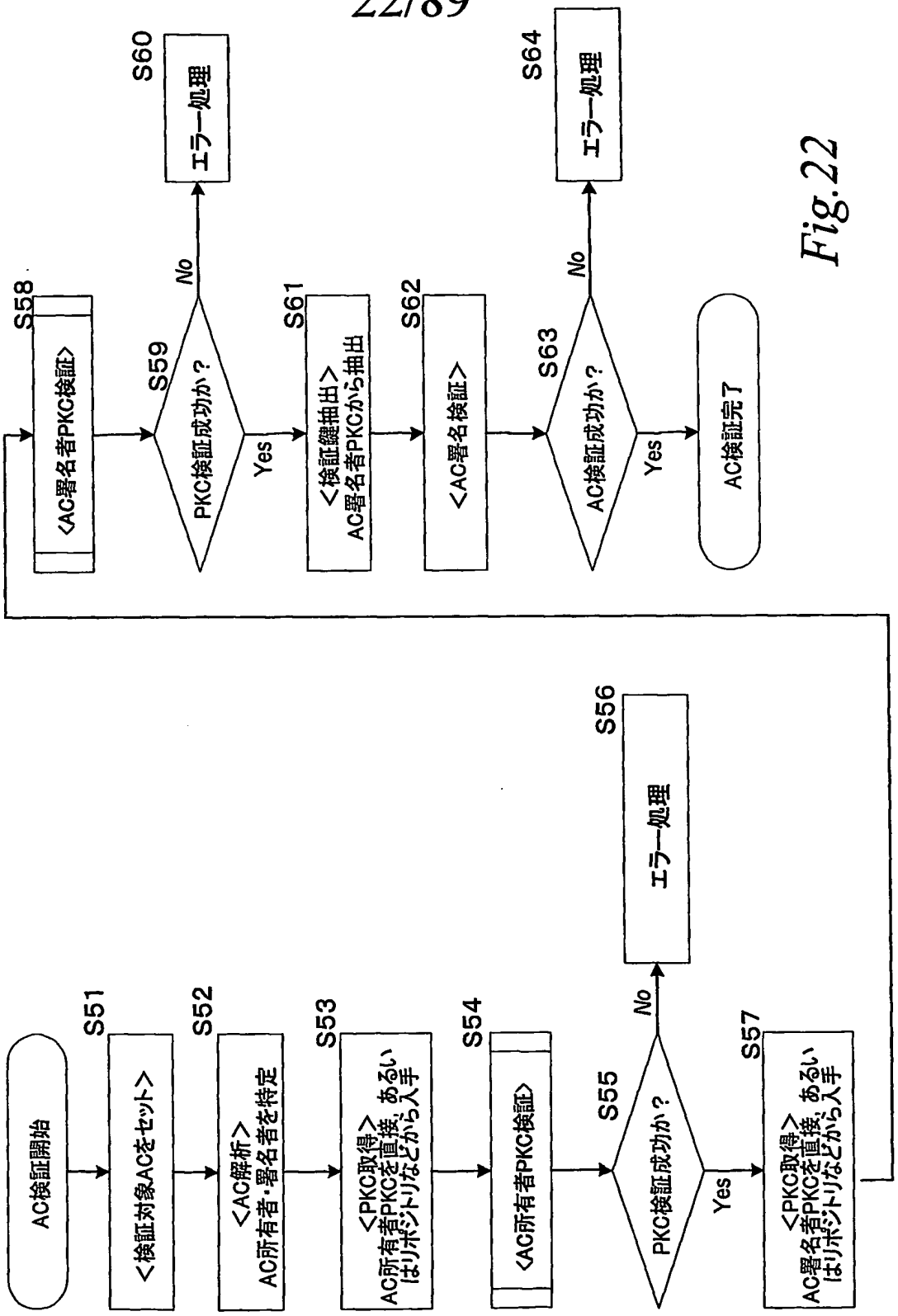

AC検証開始
S51
<検証対象ACをセット>
S52
<AC解析>
AC所有者・署名者を特定
S53
<PKC取得>
AC所有者PKCを直接、あるいはリポジトリなどから入手
S54
<AC所有者PKC検証>
S55
PKC検証成功か？
No
S56
エラー処理
Yes
S57
<PKC取得>
AC署名者PKCを直接、あるいはリポジトリなどから入手
S58
<AC署名者PKC検証>
S59
PKC検証成功か？
No
S60
エラー処理
Yes
S61
<検証鍵抽出>
AC署名者PKCから抽出
S62
<AC署名検証>
S63
AC検証成功か？
No
S64
エラー処理
Yes
AC検証完了

Fig. 22

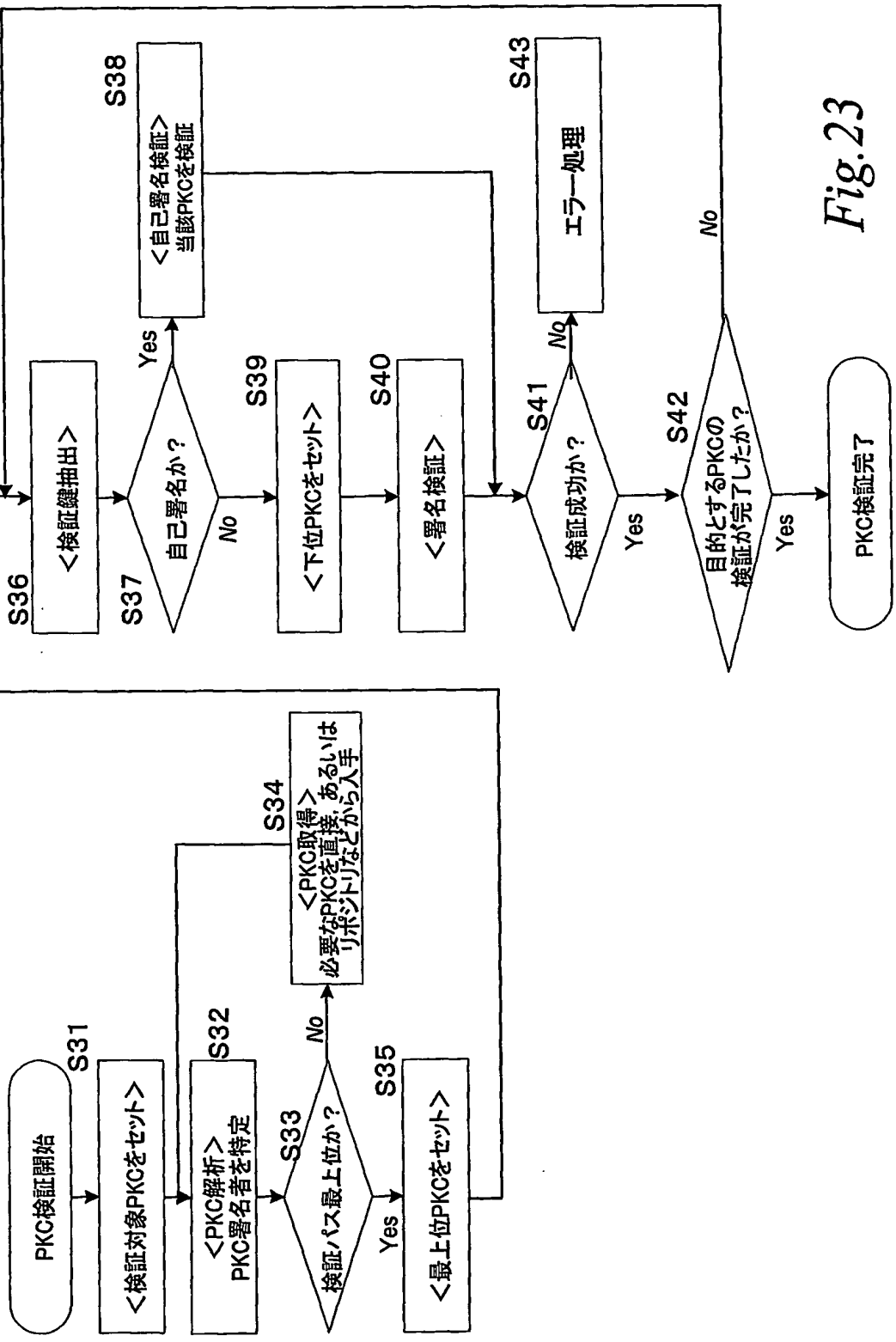
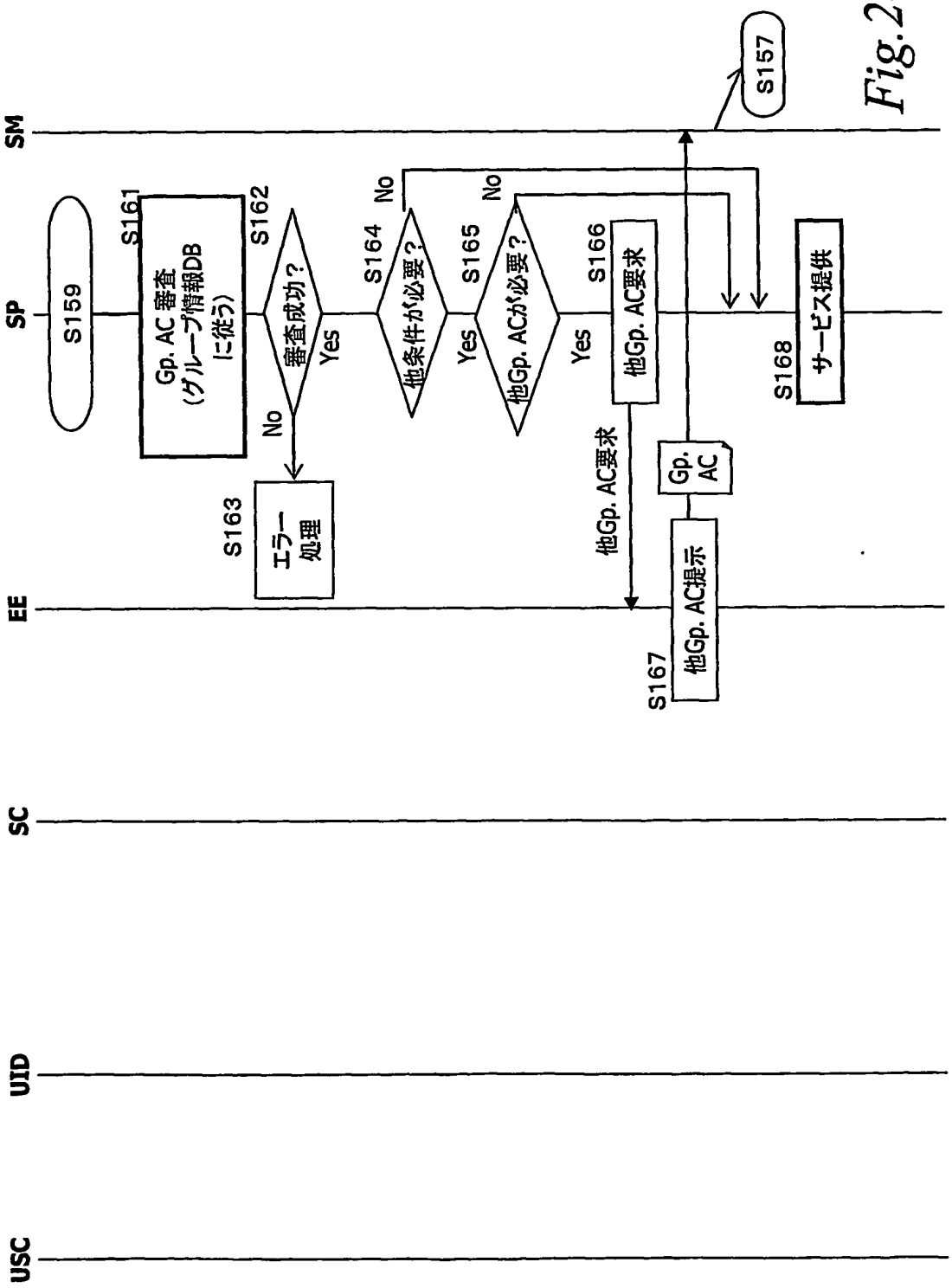

PKC検証開始
S31
<検証対象PKCをセット>
S32
<PKC解析>
PKC署名者を特定
S33
検証パス最上位か？
No
S34
<PKC取得>
必要なPKCを直接、あるいは
リポジトリなどから入手
Yes
S35
<最上位PKCをセット>
S36
<検証鍵抽出>
S37
自己署名か？
Yes
S38
<自己署名検証>
当該PKCを検証
No
S39
<下位PKCをセット>
S40
<署名検証>
S41
検証成功か？
No
S43
エラー処理
Yes
S42
目的とするPKCの
検証が完了したか？
No
Yes
PKC検証完了

Fig.23

Fig. 24


SM
SP
EE
SC
UID
USC
S157
S159
S161
Gp. AC 審査
(グループ情報DB
に従う)
S162
審査成功?
Yes
No
S163
エラー
処理
S164
他条件が必要?
No
Yes
S165
他Gp. ACが必要?
No
Yes
S166
他Gp. AC要求
S167
他Gp. AC提示
他Gp. AC要求
Gp.
AC
S168
サービス提供

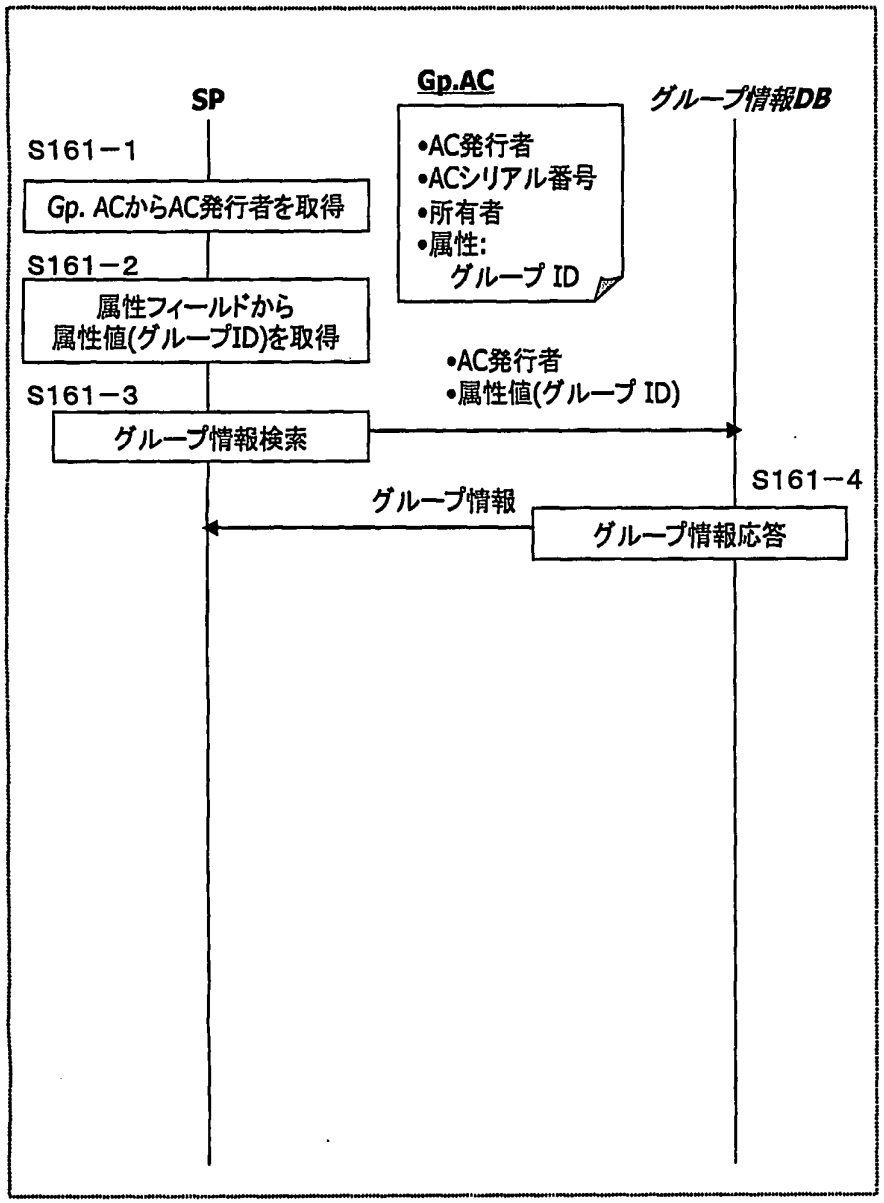


Fig.25

グループ情報DB 例

発行者	グループ ID	グループ情報
メーカー	1001	メンテナンス フルサービス加入者
メーカー	1002	メンテナンス トライアル
ゲーム配信サービス	1234-0	ゲーム配信サービス加入者
ゲーム配信サービス	1234-5-10	ゲーム10回使用ユーザ
田中家 世帯主	001	田中家 家族
田中家 世帯主	002	田中家 子供

WO 03/105400
PCT/JP03/06585

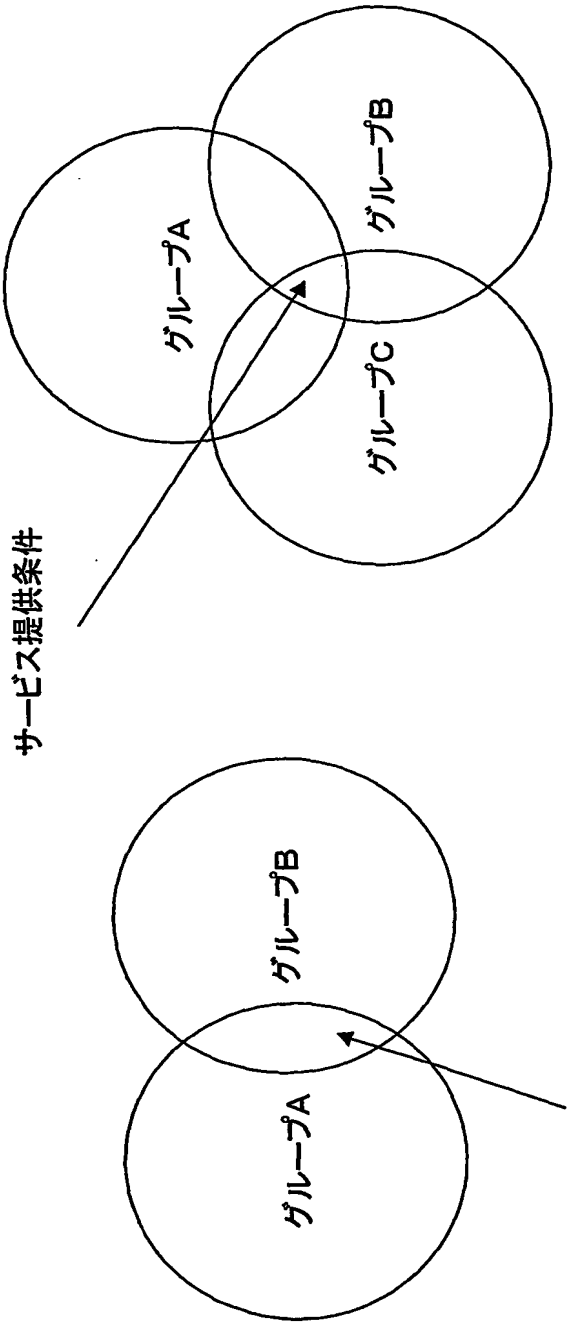


Fig.26

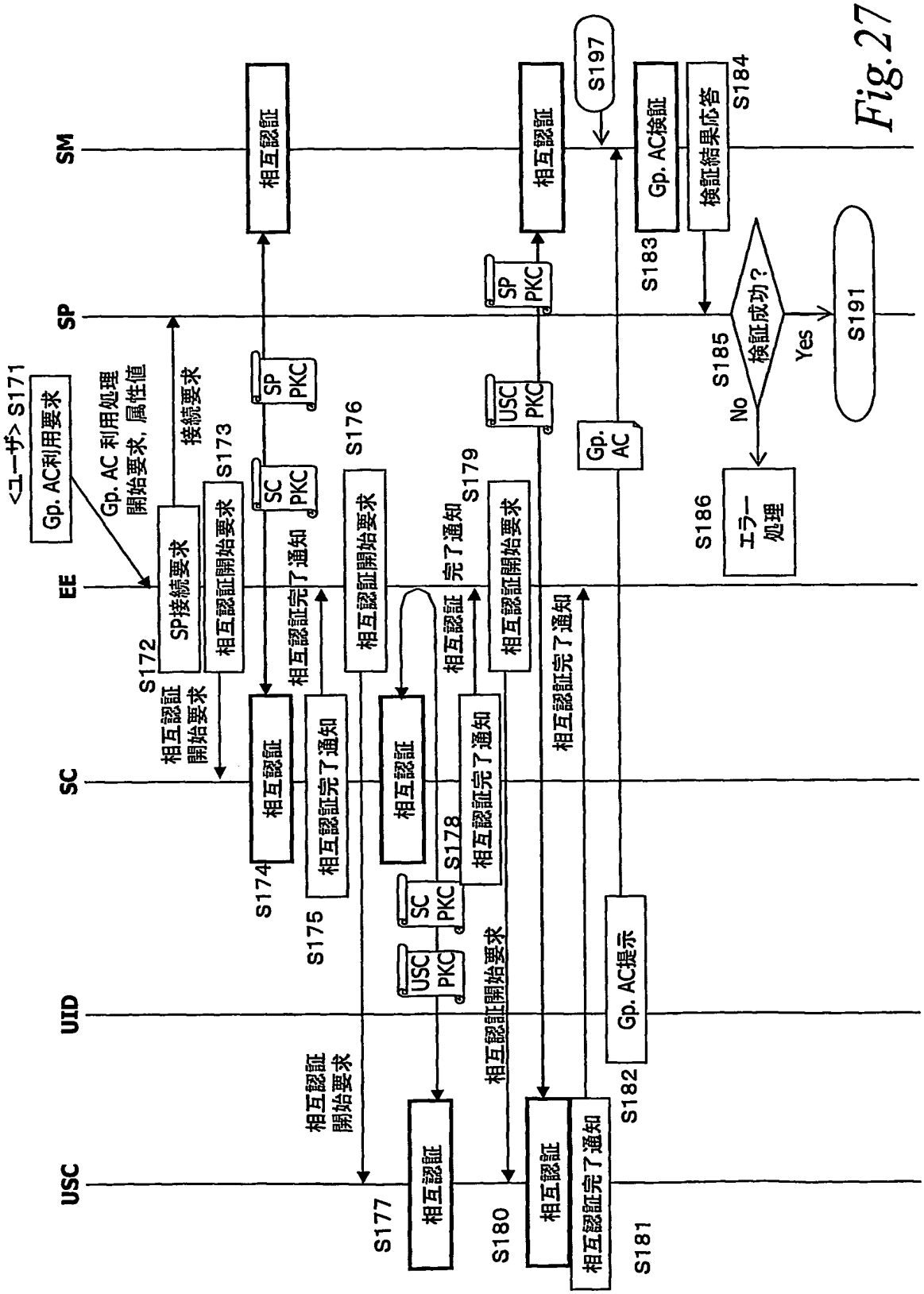

SM
SP
EE
SC
UID
USC
<ユーザ> S171
Gp. AC利用要求
Gp. AC 利用処理 開始要求, 属性値
接続要求
S172
SP接続要求
S173
相互認証開始要求
相互認証
SP PKC
SC PKC
S174
相互認証
相互認証完了通知
S175
相互認証完了通知
S176
相互認証開始要求
相互認証
SC PKC
USC PKC
S177
相互認証開始要求
相互認証
S178
相互認証完了通知
S179
相互認証開始要求
相互認証
USC PKC
SP PKC
S180
相互認証
相互認証完了通知
S181
相互認証完了通知
Gp. AC
S182
Gp. AC提示
S197
相互認証
S183
Gp. AC検証
S184
検証結果応答
S185
検証成功?
No
S186
エラー処理
Yes
S191

Fig. 27

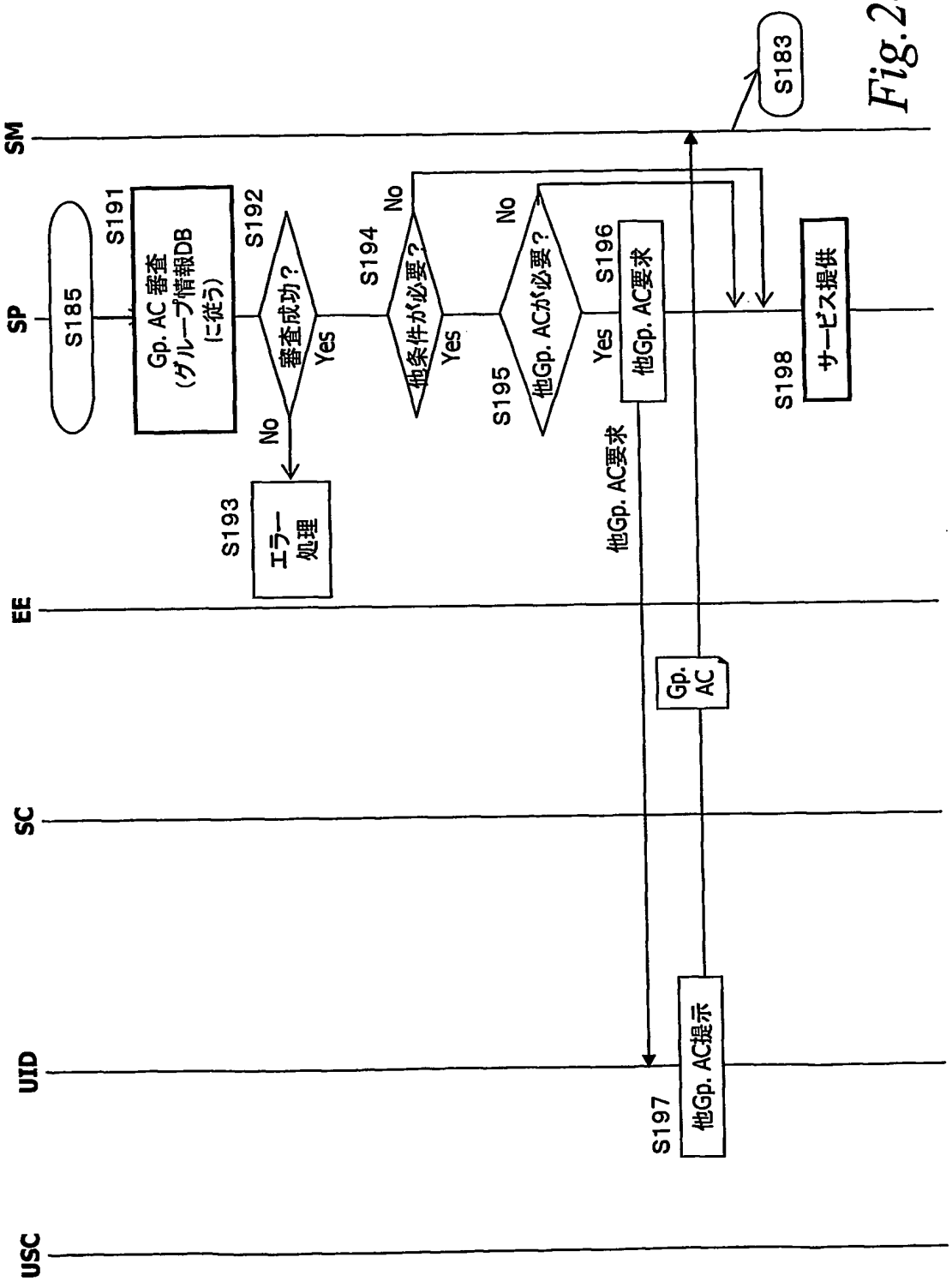

SM
SP
EE
SC
UID
USC
S185
S191
Gp. AC 審査
(グループ情報DB
に従う)
S192
審査成功?
Yes
No
S193
エラー
処理
S194
他条件が必要?
Yes
No
S195
他Gp. ACが必要?
Yes
No
S196
他Gp. AC要求
S198
サービス提供
S183
他Gp. AC要求
Gp.
AC
S197
他Gp. AC提示

Fig. 28

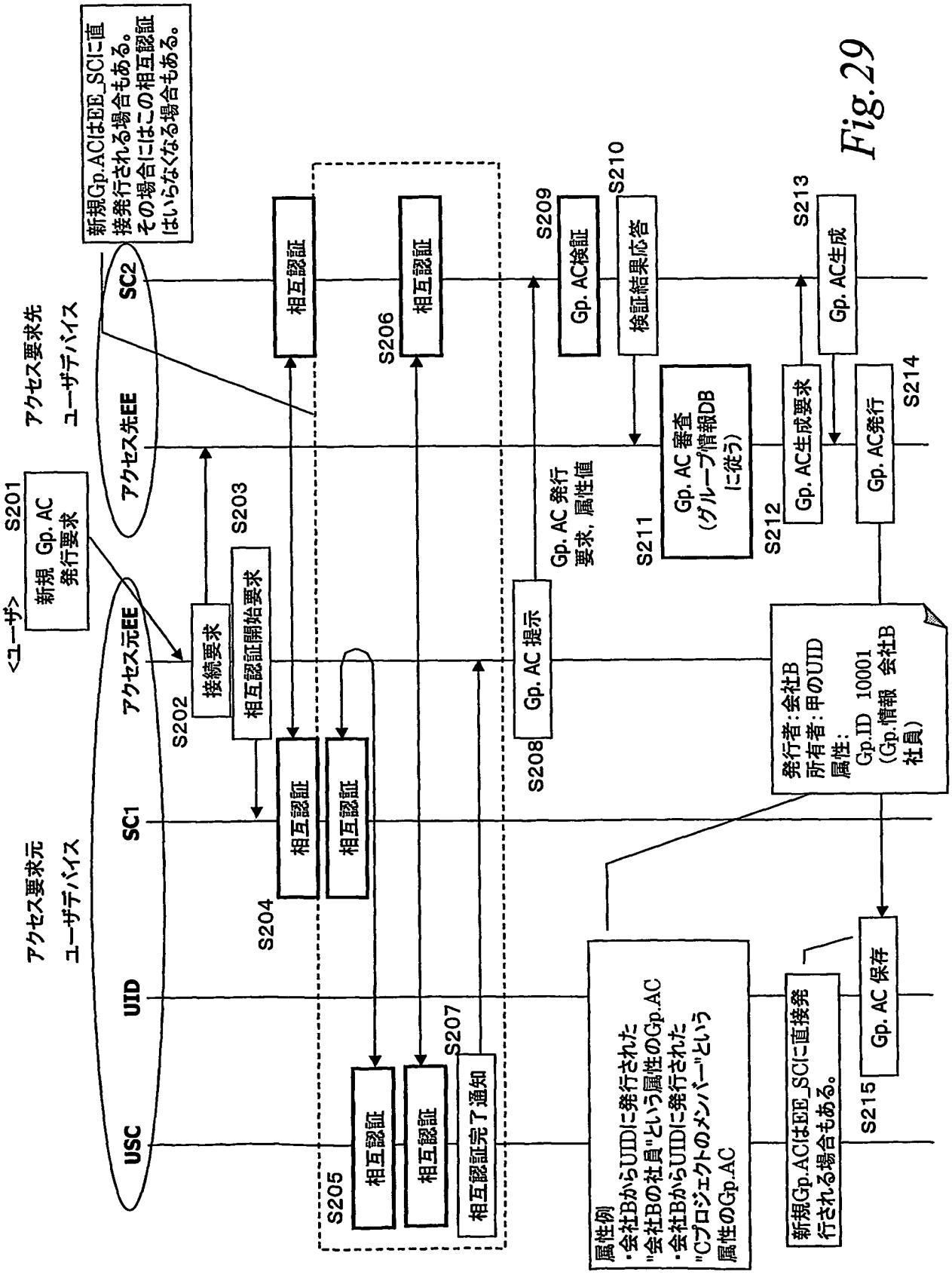

アクセス要求元
ユーザデバイス
USC
UID
SC1
SC2
アクセス元EE
アクセス先EE
アクセス先
ユーザデバイス
<ユーザ>
新規Gp.ACはEE_SCに直接発行される場合もある。その場合にはこの相互認証はいらなくなる場合もある。
S201
新規 Gp. AC 発行要求
S202
接続要求
S203
相互認証開始要求
S204
相互認証
相互認証
S205
相互認証
相互認証
S206
相互認証
相互認証
S207
相互認証完了通知
S208
Gp. AC 提示
Gp. AC 発行要求, 属性値
S209
Gp. AC検証
S210
検証結果応答
S211
Gp. AC 審査 (グループ情報DBに従う)
S212
Gp. AC生成要求
S213
Gp. AC生成
S214
Gp. AC発行
発行者:会社B
所有者:甲のUID
属性:
Gp.ID 10001
(Gp.情報 会社B社員)
属性例
・会社BからUIDに発行された"会社Bの社員"という属性のGp.AC
・会社BからUIDに発行された"Cプロジェクトのメンバー"という属性のGp.AC
新規Gp.ACはEE_SCに直接発行される場合もある。
S215
Gp. AC 保存

Fig.29

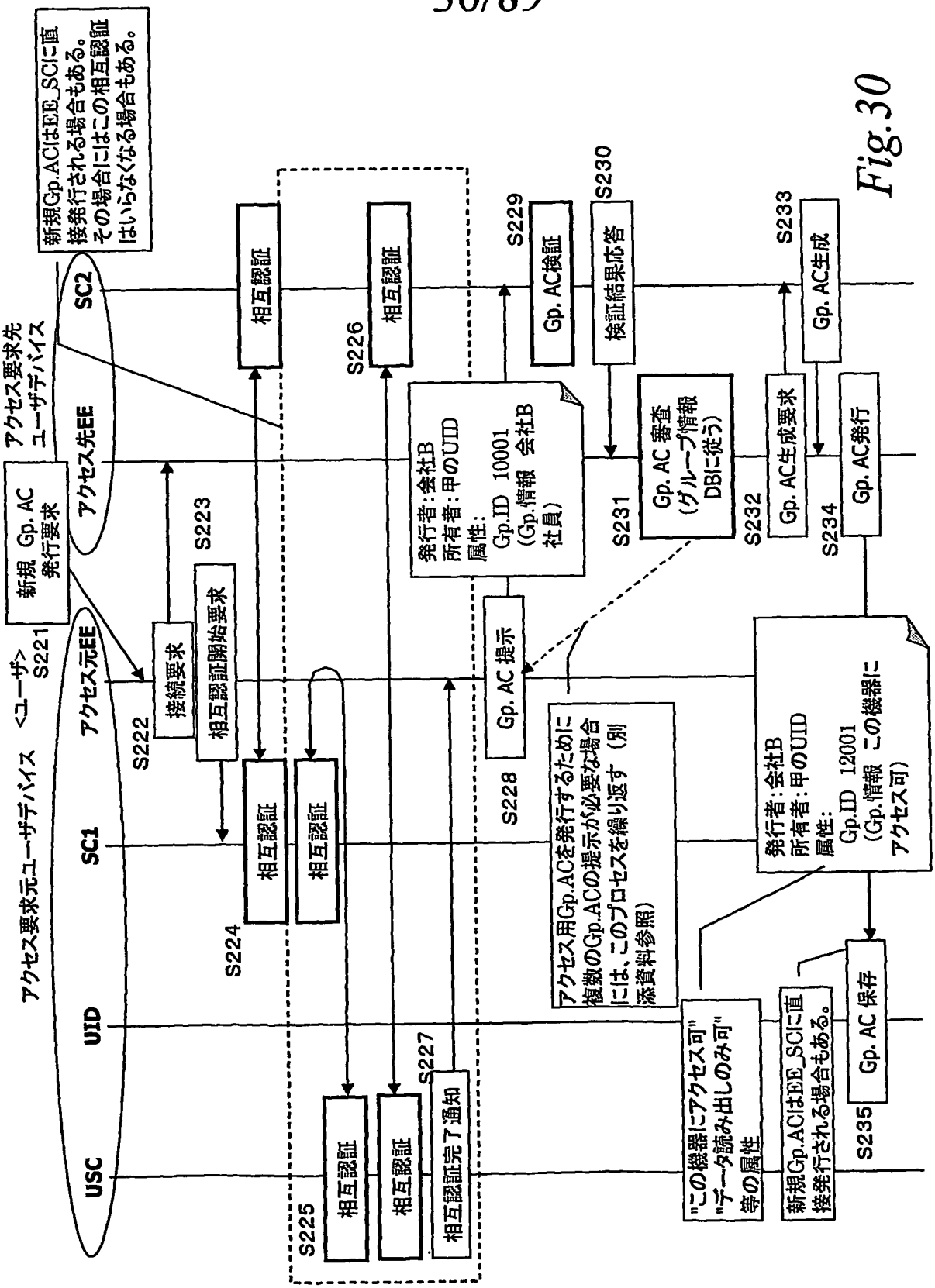
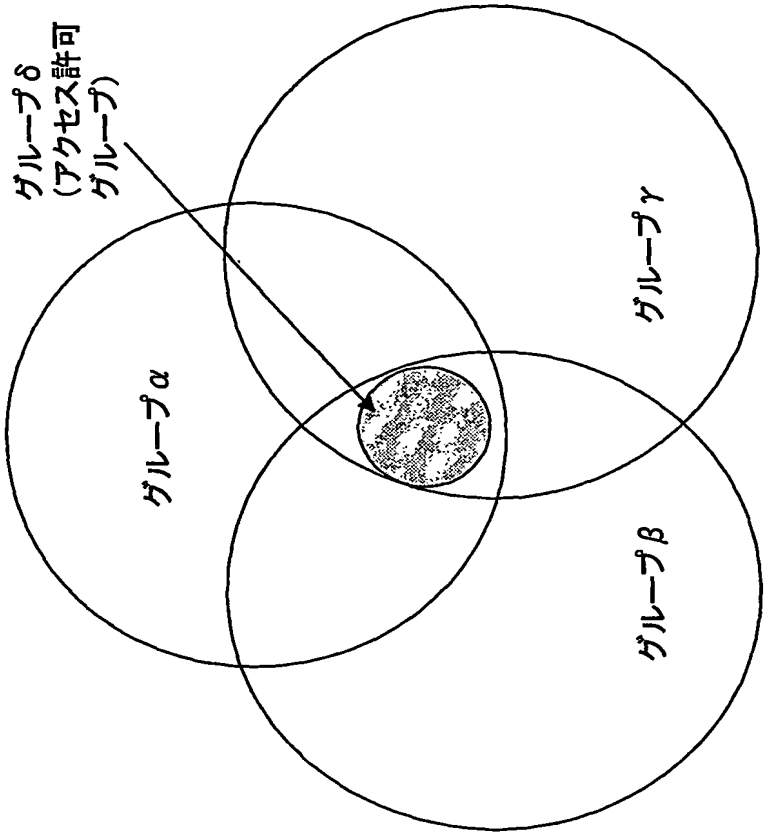
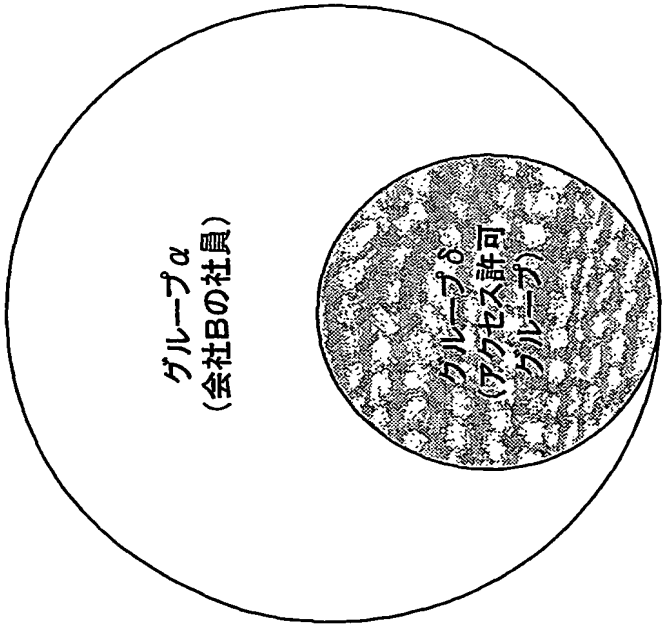

アクセス要求元ユーザデバイス
<ユーザ>
UID
USC
SC1
SC2
アクセス元EE
アクセス先EE
アクセス要求先
ユーザデバイス
新規 Gp. AC
発行要求
S221
接続要求
S222
相互認証開始要求
S223
相互認証
S224
相互認証
相互認証
相互認証
S225
相互認証
相互認証
S226
相互認証完了通知
S227
Gp. AC 提示
S228
発行者:会社B
所有者:甲のUID
属性:
Gp.ID 10001
(Gp.情報 会社B
社員)
S229
Gp. AC検証
S230
検証結果応答
Gp. AC 審査
(グループ情報
DBに従う)
S231
Gp. AC生成要求
S232
S233
Gp. AC生成
Gp. AC発行
S234
発行者:会社B
所有者:甲のUID
属性:
Gp.ID 12001
(Gp.情報 この機器に
アクセス可)
Gp. AC 保存
S235
新規Gp.ACはEE_SCに直
接発行される場合もある。
その場合にはこの相互認証
はいらなくなる場合もある。
アクセス用Gp.ACを発行するために
複数のGp.ACの提示が必要な場合
には、このプロセスを繰り返す（別
添資料参照）
"この機器にアクセス可"
"データ読み出しのみ可"
等の属性
新規Gp.ACはEE_SCに直
接発行される場合もある。

Fig. 30


グループδ
(アクセス許可
グループ)
グループα
グループγ
グループβ

(b)


グループα
(会社Bの社員)
グループδ
(アクセス許可
グループ)

(a)

Fig.31

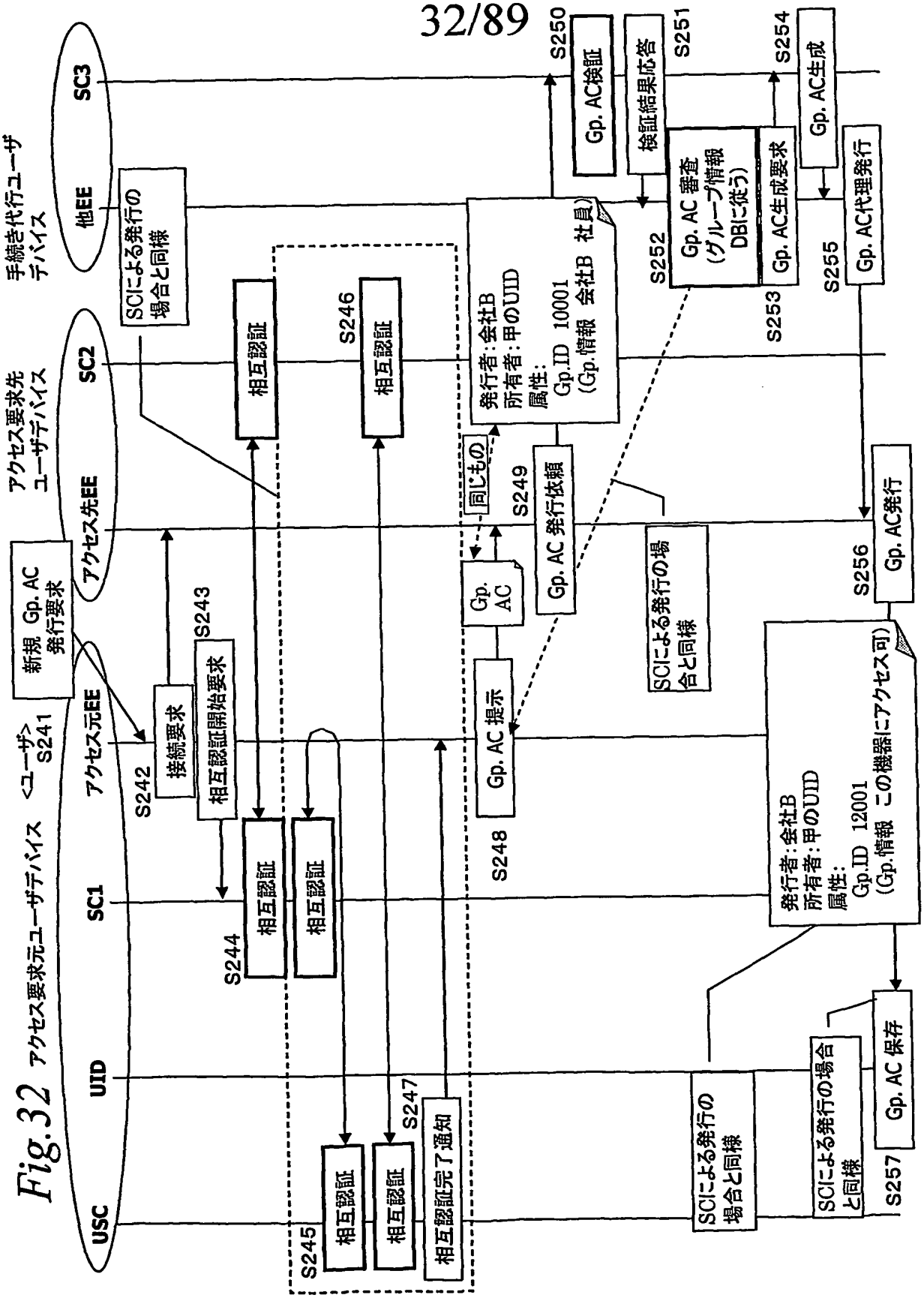


Fig.32 アクセス要求元ユーザデバイス

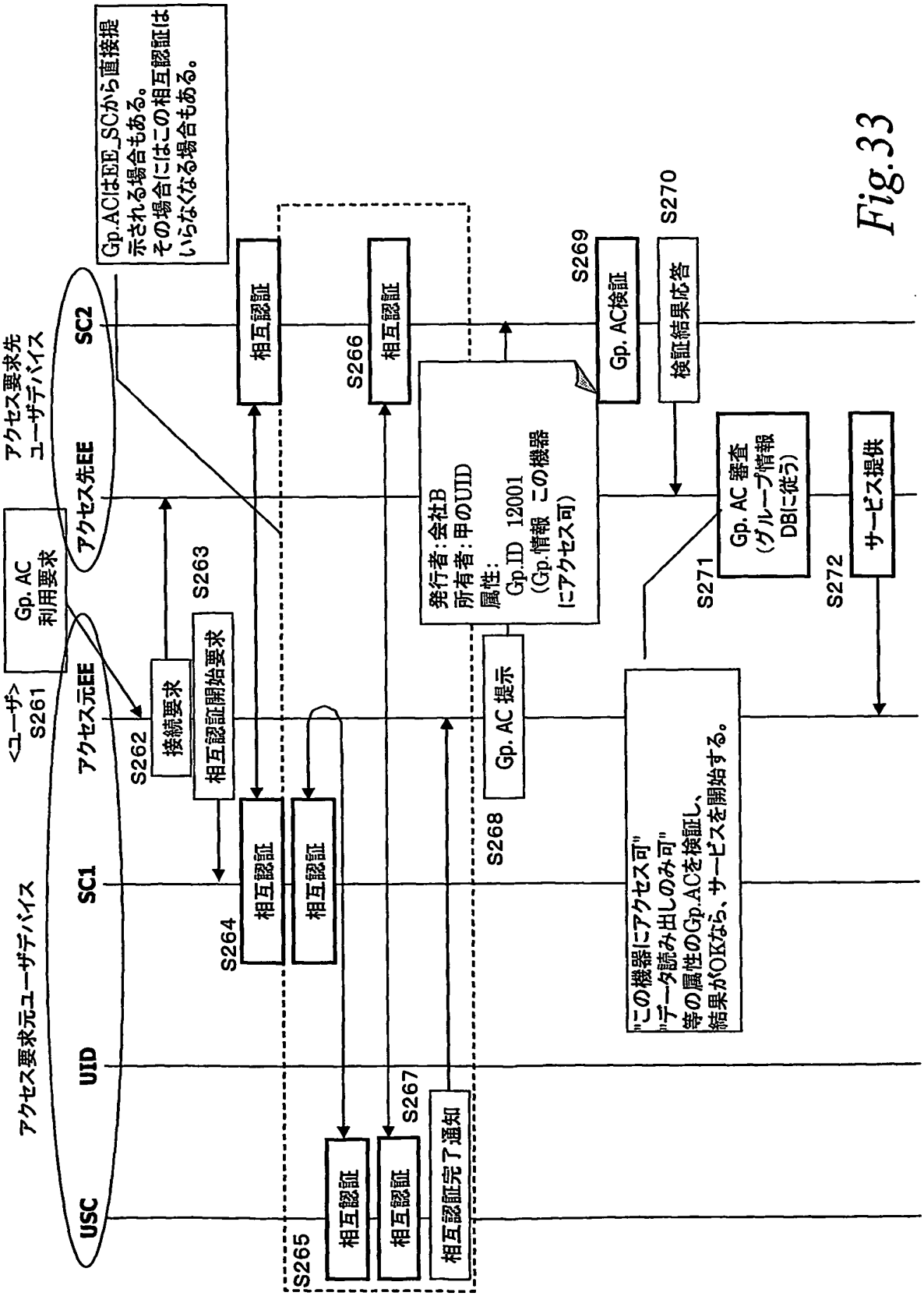

アクセス要求元ユーザデバイス
USC
UID
SC1
アクセス元EE
<ユーザ>
S261
Gp. AC
利用要求
アクセス先EE
アクセス要求先
ユーザデバイス
SC2
Gp.ACはEE_SCから直接提示される場合もある。
その場合にはこの相互認証はいらなくなる場合もある。
S262
接続要求
S263
相互認証開始要求
S264
相互認証
相互認証
相互認証
S265
相互認証
相互認証
S267
相互認証完了通知
S266
相互認証
S268
Gp. AC 提示
発行者:会社B
所有者:甲のUID
属性:
Gp.ID 12001
(Gp.情報 この機器にアクセス可)
S269
Gp. AC検証
S270
検証結果応答
S271
Gp. AC 審査
(グループ情報DBに従う)
S272
サービス提供
"この機器にアクセス可"
"データ読み出しのみ可"
等の属性のGp.ACを検証し、
結果がOKなら、サービスを開始する。

Fig. 33

発行者	発行タイミング	所有者	検証者	属性
カード会社A	任意 （EE購入前でも可）	甲さんUID_USC	SP_SM	カード会社A 会員
会社B	任意 （EE購入前でも可）	甲さんUID_USC	SP_SM	会社B 社員
役所	任意 （EE購入前でも可）	家族各UID_USC	SP_SM	甲さんの家族
甲さん	任意 （EE購入前でも可）	家族各UID_USC	SP_SM	甲さんの家族
EEメーカーC	EE購入時	甲さんUID_USC	SP_SM	EE ユーザ登録
EEメーカーC	EE製造時	機器EE_SC	SP_SM	EE EE登録
甲さん	EE購入後	機器EE_SC	SP_SM	発行者の所有物
EEメーカーC	EE購入後	機器EE_SC	SP_SM	甲さんの機器

Fig.34

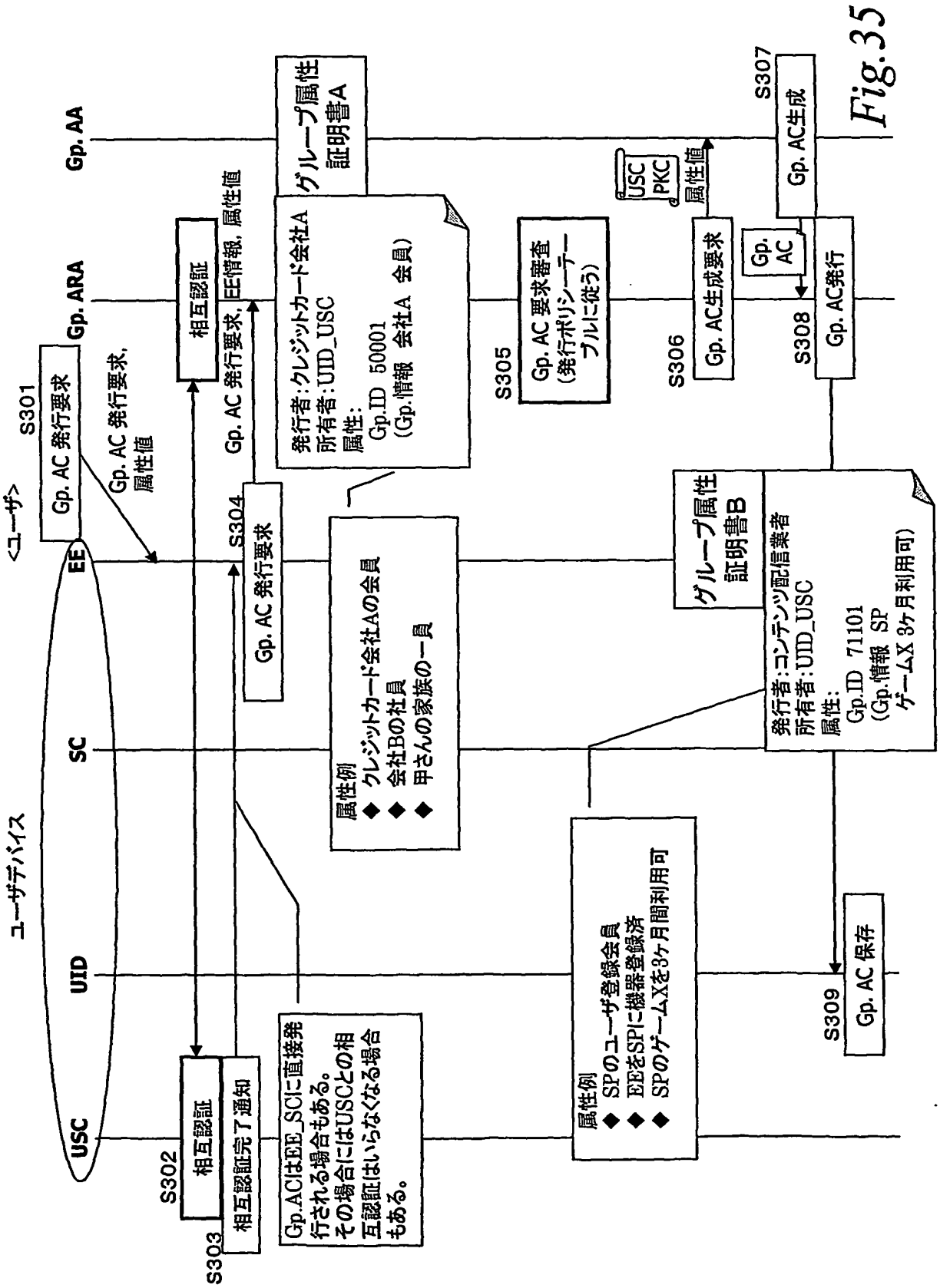

ユーザデバイス
USC
UID
SC
EE
Gp. ARA
Gp. AA
<ユーザ>
S301
Gp. AC 発行要求
Gp. AC 発行要求, 属性値
S302
相互認証
S303
相互認証完了通知
Gp. AC 発行要求, EE情報, 属性値
相互認証
S304
Gp. AC 発行要求
Gp.ACはEE_SCに直接発行される場合もある。その場合にはUSCとの相互認証はいらなくなる場合もある。
発行者:クレジットカード会社A
所有者:UID_USC
属性:
Gp.ID 50001
(Gp.情報 会社A 会員)
属性例
◆ クレジットカード会社Aの会員
◆ 会社Bの社員
◆ 甲さんの家族の一員
グループ属性証明書A
S305
Gp. AC 要求審査
(発行ポリシーテーブルに従う)
S306
Gp. AC生成要求
USC
PKC
属性値
S307
Gp. AC生成
Gp. AC
S308
Gp. AC発行
グループ属性証明書B
発行者:コンテンツ配信業者
所有者:UID_USC
属性:
Gp.ID 71101
(Gp.情報 SP
ゲームX 3ヶ月利用可)
属性例
◆ SPのユーザ登録会員
◆ EEをSPに機器登録済
◆ SPのゲームXを3ヶ月間利用可
S309
Gp. AC 保存

Fig. 35

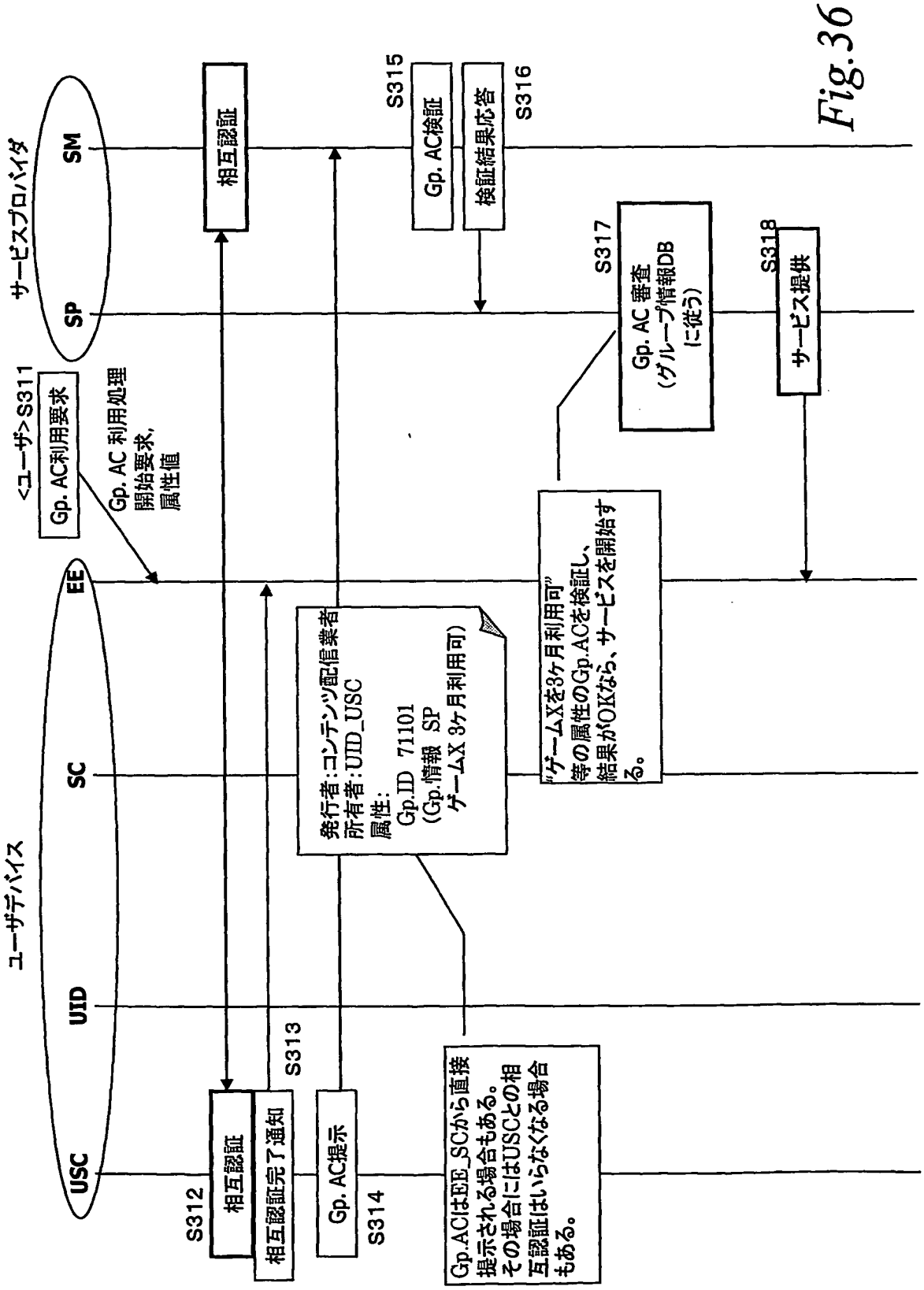

ユーザデバイス
USC
UID
SC
EE
サービスプロバイダ
SP
SM
<ユーザ>S311
Gp. AC利用要求
Gp. AC 利用処理
開始要求,
属性値
相互認証
S312
相互認証完了通知
S313
Gp. AC提示
S314
Gp.ACはEE_SCから直接
提示される場合もある。
その場合にはUSCとの相
互認証はいらなくなる場合
もある。
発行者:コンテンツ配信業者
所有者:UID_USC
属性:
Gp.ID 71101
(Gp.情報 SP
ゲームX 3ヶ月利用可)
S315
Gp. AC検証
検証結果応答
S316
"ゲームXを3ヶ月利用可"
等の属性のGp.ACを検証し、
結果がOKなら、サービスを開始す
る。
S317
Gp. AC 審査
(グループ情報DB
に従う)
S318
サービス提供

Fig.36

	AC名称	属性情報 (＝発行ポリシー)	発行者(グループ AA,ARA)	所有者
AC01	1. 学生証	発行者の学生である	A大学(の運営(管理) するAA)	ユーザC君のUIDの USC
AC02	2. 美術講座受講証	発行者の開催する美術 講座受講権利者である	A大学(の運営(管理) するAA)	ユーザC君のUIDの USC
AC03	3. 管理機器証明書	発行者の管理する機器 である	A大学(の運営(管理) するAA)	エンドエンティティ(EE) としてのテレビDのSC
AC04	4. 教育用機器証明書	教育使用目的の機器で ある。	文部科学省(の運営 (管理)するAA)	エンドエンティティ(EE) としてのテレビDのSC

Fig.37

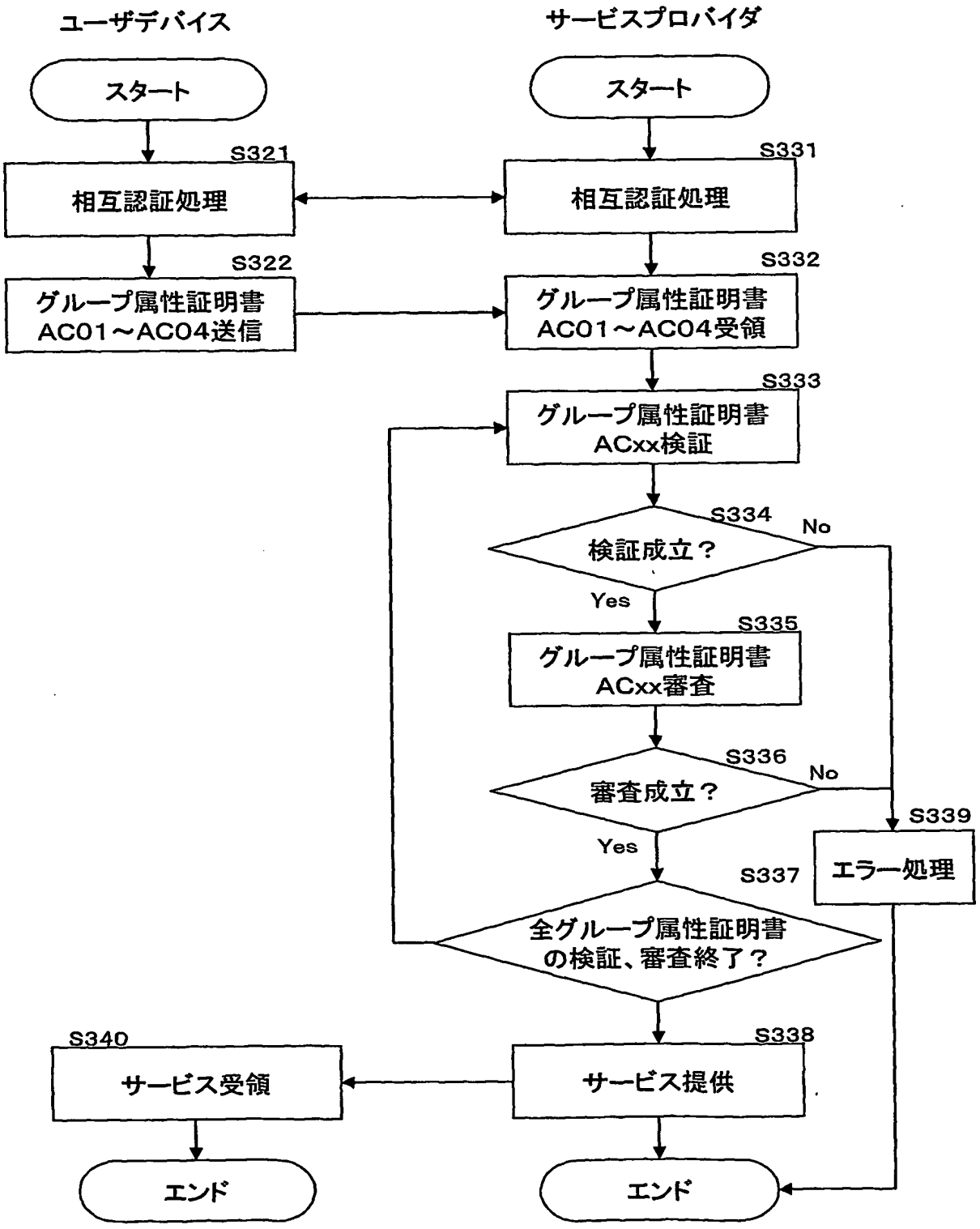
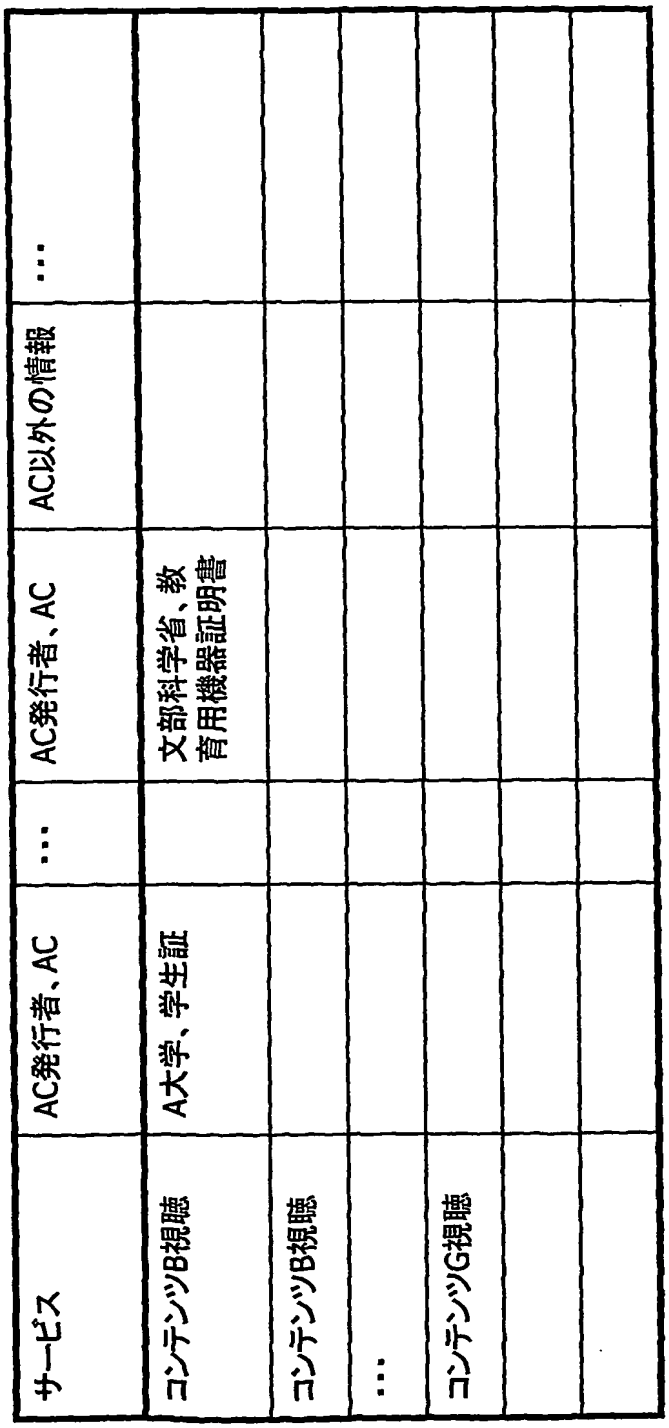

ユーザデバイス
サービスプロバイダ
スタート
スタート
S321
相互認証処理
S331
相互認証処理
S322
グループ属性証明書
AC01～AC04送信
S332
グループ属性証明書
AC01～AC04受領
S333
グループ属性証明書
ACxx検証
S334
検証成立？
No
Yes
S335
グループ属性証明書
ACxx審査
S336
審査成立？
No
S339
エラー処理
Yes
S337
全グループ属性証明書
の検証、審査終了？
S340
サービス受領
S338
サービス提供
エンド
エンド

Fig.38



サービス	AC発行者、AC	・・・	AC発行者、AC	AC以外の情報	・・・
コンテンツB視聴	A大学、学生証		文部科学省、教育用機器証明書		
コンテンツB視聴					
・・・					
コンテンツG視聴					

Fig.39

(a)
グループAC01
学生証
グループAC02
美術講座受講証
ユーザ条件(UIDのUSC対応の
グループ属性証明書によって確認)
(b)
グループAC03
管理機器証明書
グループAC04
教育用機器
証明書
機器条件(EEのSC対応の
グループ属性証明書によって確認)

Fig. 40

	発行者	所有者	検証者	属性
AC01	病院側 医療機器(SP)	甲さんUID_USC or EE_SC	病院側医療機器 (SP_SM)	プログラムE実行可
AC02	自宅側医療機器 (EE)	病院側医療機器 (SP_SM)	自宅側医療機器 (EE_SC)	データXの引き取り処 理可

Fig.41

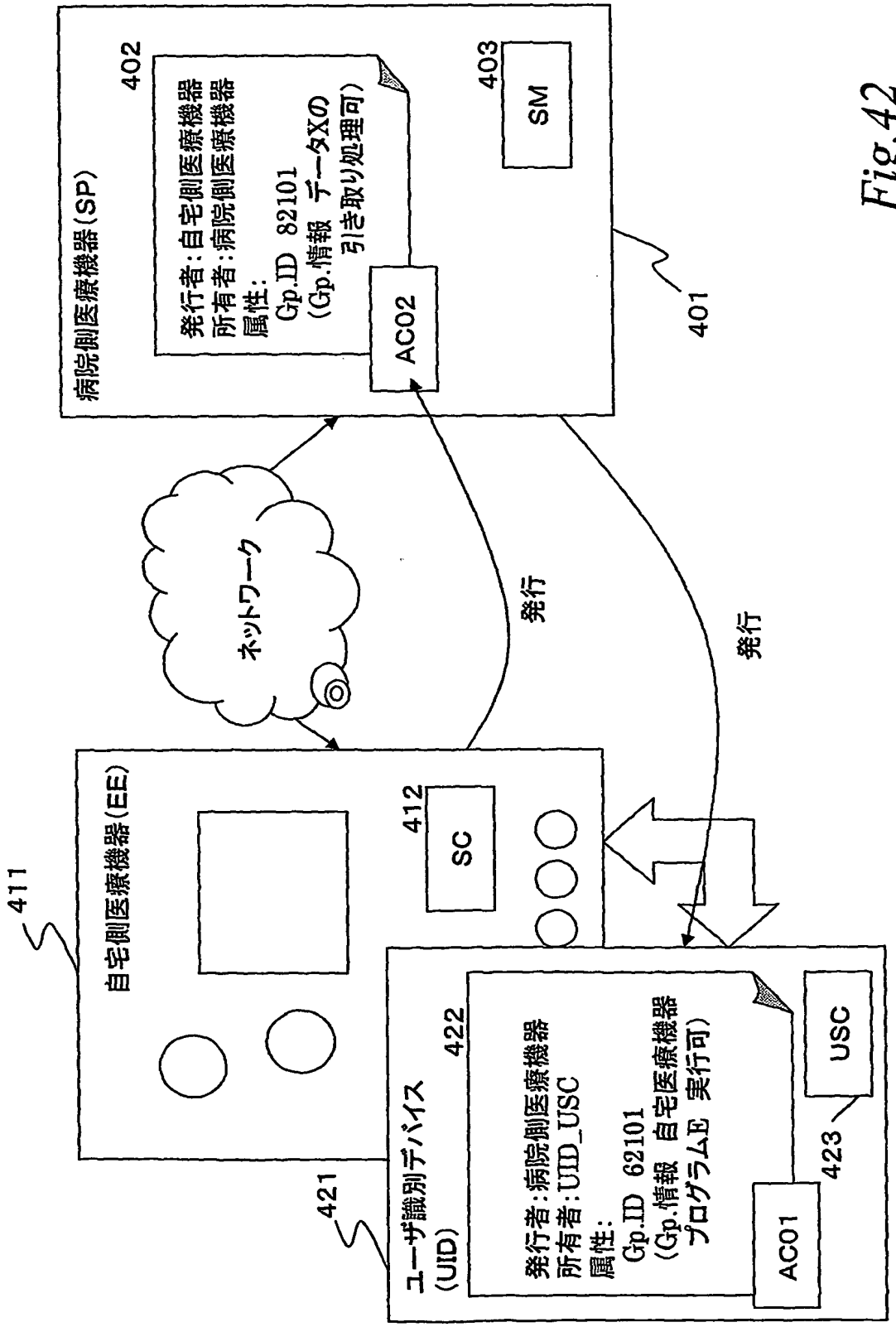

病院側医療機器(SP)
402
発行者:自宅側医療機器
所有者:病院側医療機器
属性:
Gp.ID 82101
(Gp.情報 データXの
引き取り処理可)
AC02
403
SM
401
ネットワーク
発行
発行
411
自宅側医療機器(EE)
412
SC
421
ユーザ識別デバイス
(UID)
422
発行者:病院側医療機器
所有者:UID_USC
属性:
Gp.ID 62101
(Gp.情報 自宅医療機器
プログラムE 実行可)
USC
423
AC01

Fig.42

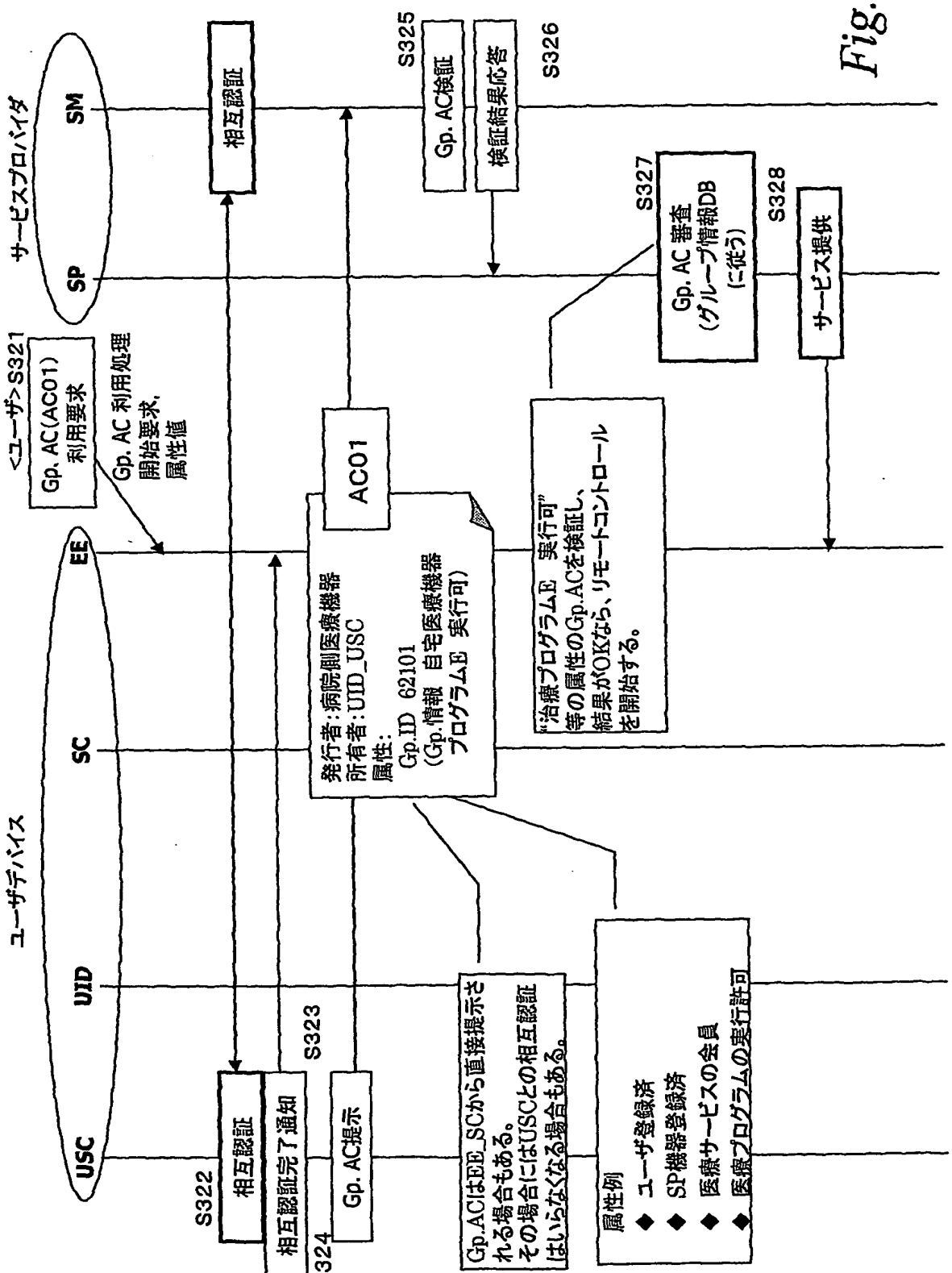
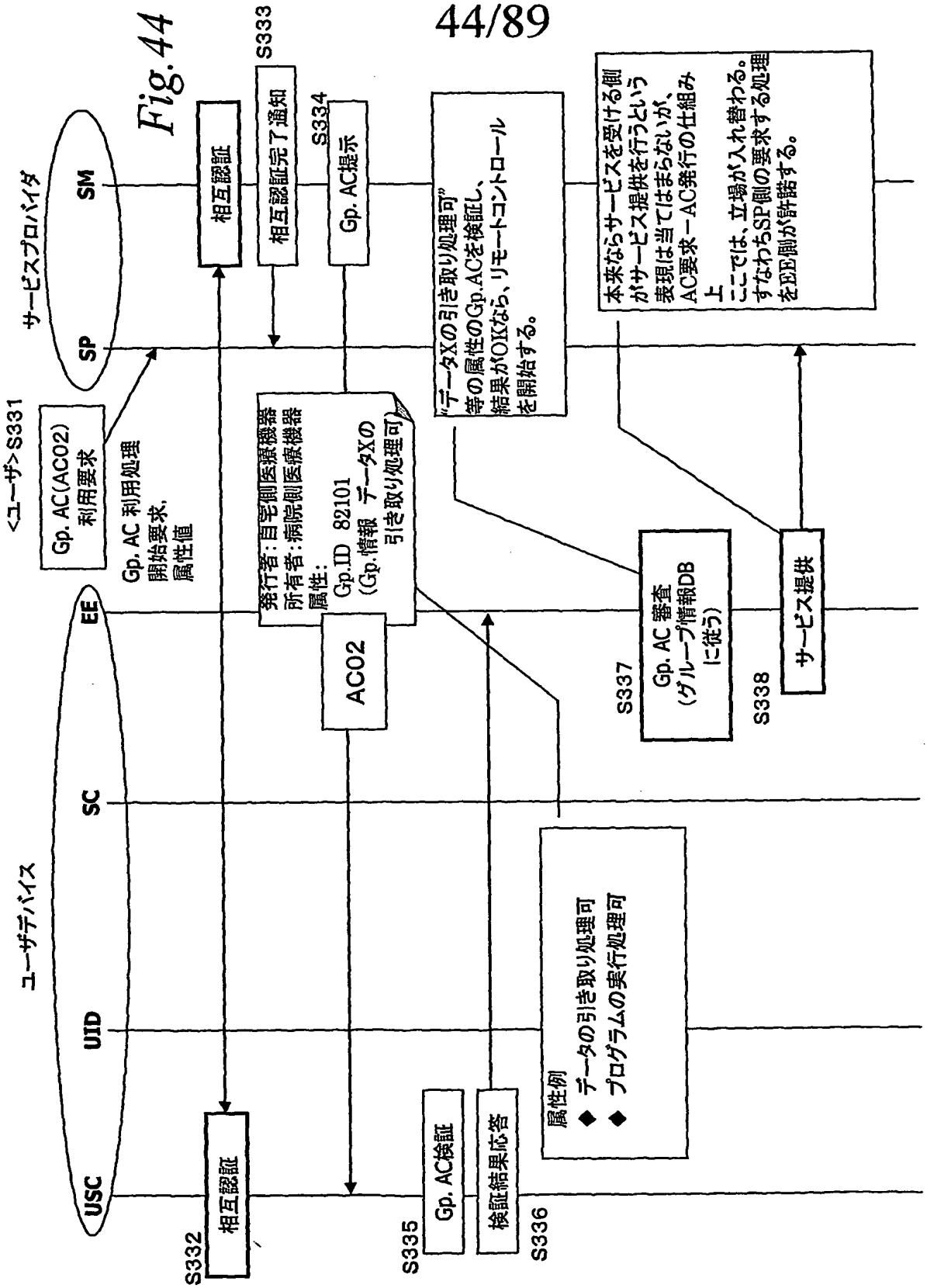

ユーザデバイス
USC
UID
SC
EE
サービスプロバイダ
SP
SM
<ユーザ>S321
Gp. AC(AC01)
利用要求
Gp. AC 利用処理
開始要求,
属性値
相互認証
S322
相互認証完了通知
S323
S324
Gp. AC提示
発行者:病院側医療機器
所有者:UID_USC
属性:
Gp.ID 62101
(Gp.情報 自宅医療機器
プログラムE 実行可)
AC01
Gp.ACはEE_SCから直接提示される場合もある。
その場合にはUSCとの相互認証はいらなくなる場合もある。
属性例
◆ ユーザ登録済
◆ SP機器登録済
◆ 医療サービスの会員
◆ 医療プログラムの実行許可
相互認証
S325
Gp. AC検証
検証結果応答
S326
S327
Gp. AC 審査
(グループ情報DB
に従う)
S328
サービス提供
"治療プログラムE 実行可"
等の属性のGp.ACを検証し、
結果がOKなら、リモートコントロール
を開始する。

Fig.43

Fig.44


ユーザデバイス
USC
UID
SC
EE
サービスプロバイダ
SP
SM
<ユーザ>S331
Gp. AC(AC02)
利用要求
Gp. AC 利用処理
開始要求,
属性値
相互認証
S332
相互認証
S333
相互認証完了通知
S334
Gp. AC提示
発行者:自宅側医療機器
所有者:病院側医療機器
属性:
Gp.ID 82101
(Gp.情報 データXの
引き取り処理可)
AC02
Gp. AC検証
S335
検証結果応答
S336
"データXの引き取り処理可"
等の属性のGp.ACを検証し、
結果がOKなら、リモートコントロール
を開始する。
属性例
◆ データの引き取り処理可
◆ プログラムの実行処理可
S337
Gp. AC 審査
(グループ情報DB
に従う)
S338
サービス提供
本来ならサービスを受ける側
がサービス提供を行うという
表現は当てはまらないが、
AC要求－AC発行の仕組み
上
ここでは、立場が入れ替わる。
すなわちSP側の要求する処理
を正側が許諾する。

	発行者	発行タイミング	所有者	検証者	属性
サービスAC	家電機器メーカー(SP)	家電機器購入時	甲さん UID_USC or EE_SC	SP_SM	EE メンテナンス サービス内容
コントロールAC	家電機器(EE)	事前or自動メンテナンス時	SP_SM	EE_SC	家電機器 コントロール制限 範囲X

Fig. 45

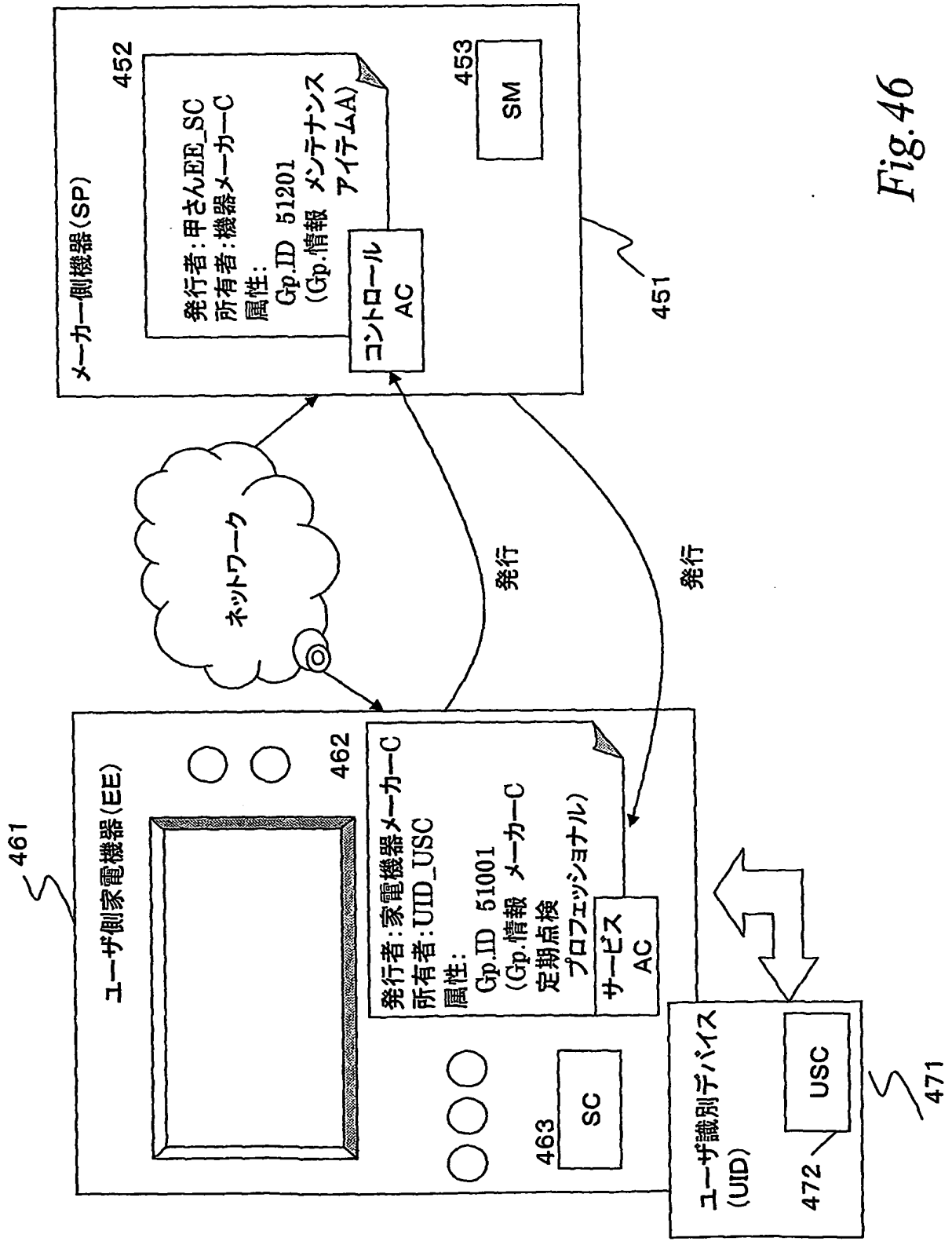

メーカー側機器(SP)
452
発行者:甲さんEE_SC
所有者:機器メーカーC
属性:
Gp.ID 51201
(Gp.情報 メンテナンス
アイテムA)
コントロール
AC
453
SM
451
ネットワーク
発行
発行
461
ユーザ側家電機器(EE)
462
発行者:家電機器メーカーC
所有者:UID_USC
属性:
Gp.ID 51001
(Gp.情報 メーカーC
定期点検
プロフェッショナル)
サービス
AC
463
SC
ユーザ識別デバイス
(UID)
472
USC
471

Fig. 46

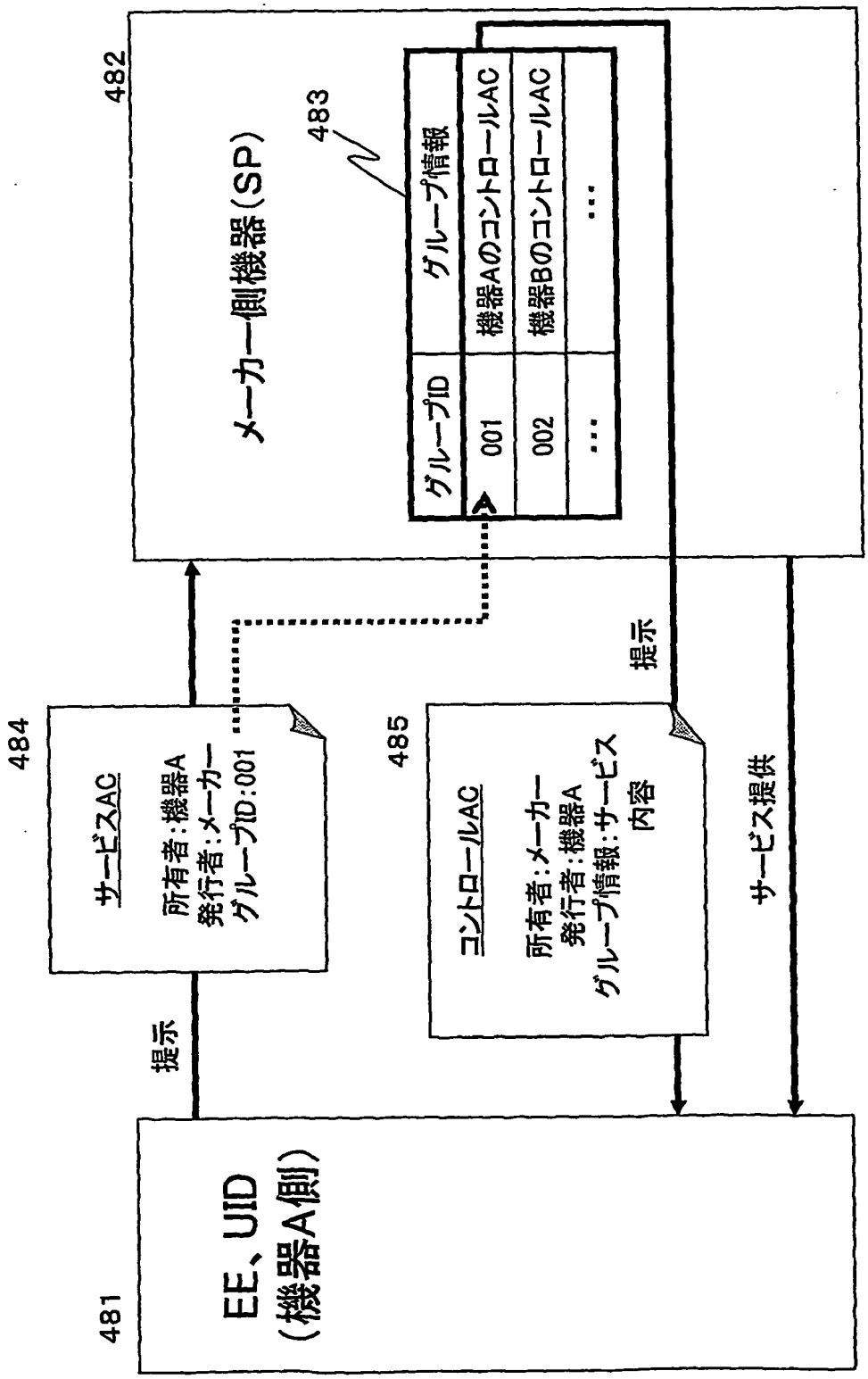
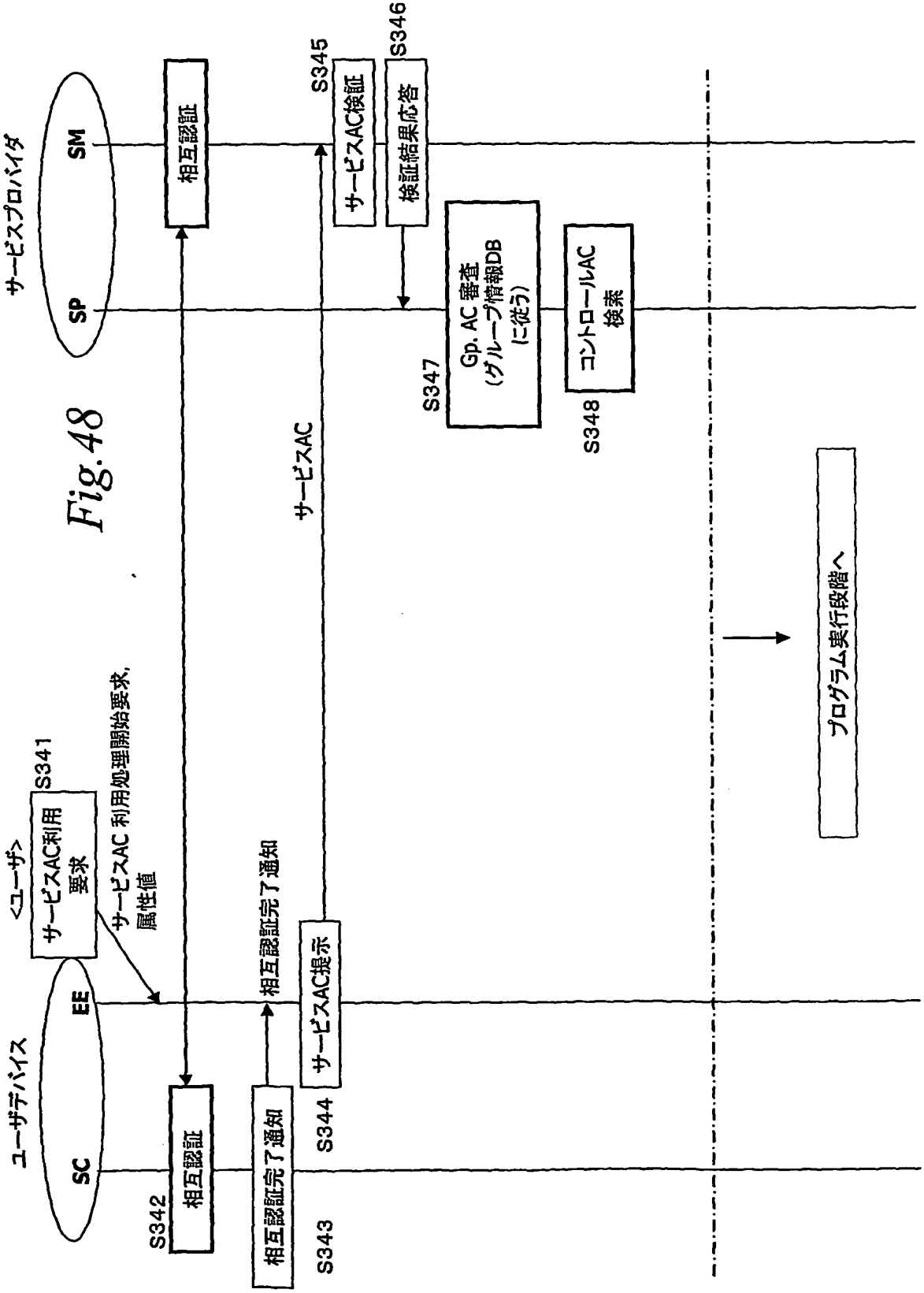

482
メーカー側機器(SP)
483
グループID
グループ情報
001
002
機器AのコントロールAC
機器BのコントロールAC
484
サービスAC
所有者:機器A
発行者:メーカー
グループID:001
485
コントロールAC
所有者:メーカー
発行者:機器A
グループ情報:サービス内容
提示
提示
サービス提供
481
EE、UID
(機器A側)

Fig.47

Fig. 48


ユーザデバイス
SC
EE
サービスプロバイダ
SP
SM
<ユーザ>
サービスAC利用要求
S341
サービスAC 利用処理開始要求,
属性値
相互認証
S342
相互認証
相互認証完了通知
S343
相互認証完了通知
サービスAC提示
S344
サービスAC
サービスAC検証
S345
検証結果応答
S346
Gp. AC 審査
(グループ情報DBに従う)
S347
コントロールAC検索
S348
プログラム実行段階へ

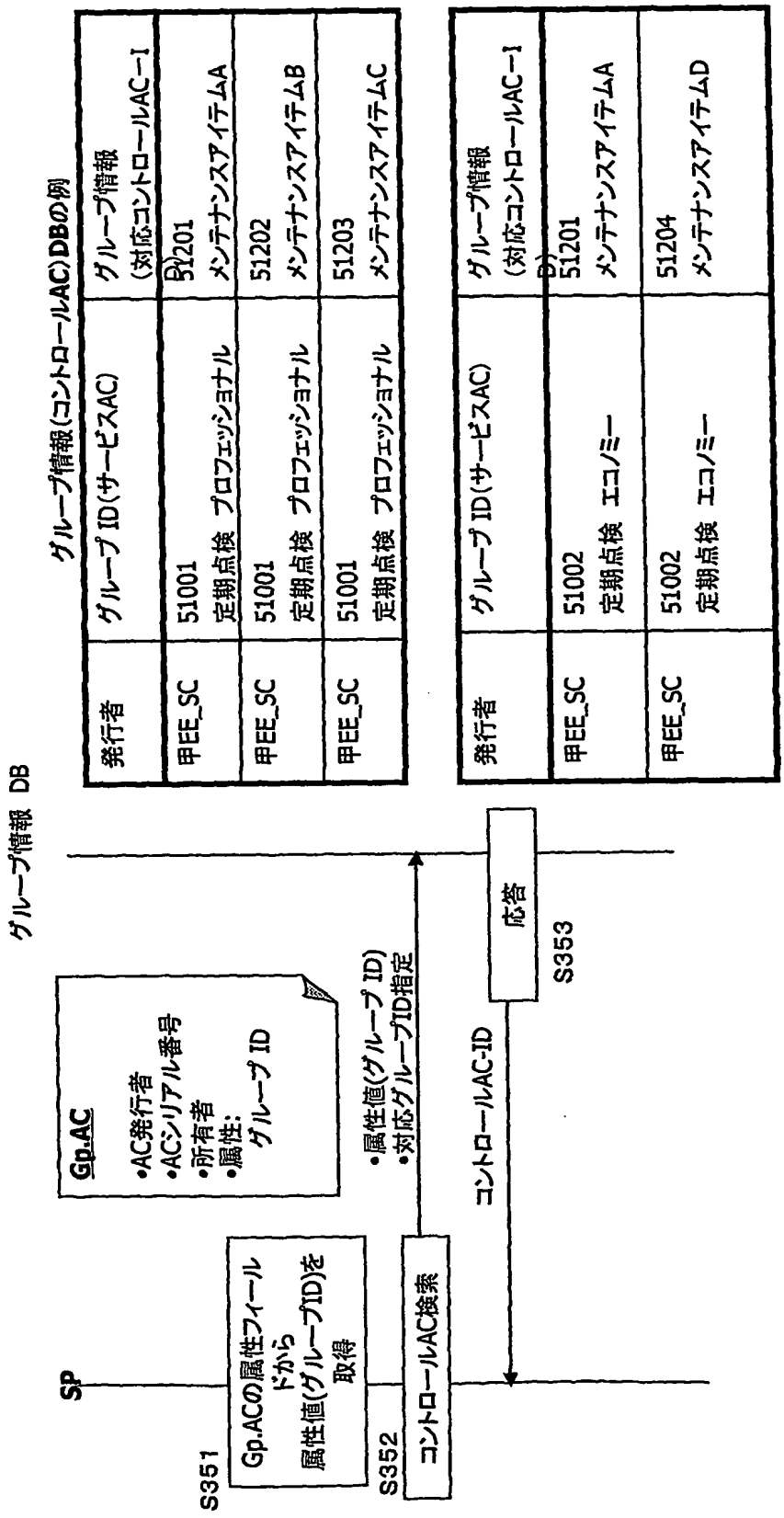

グループ情報 DB
SP
S351
Gp.ACの属性フィールドから属性値(グループID)を取得
S352
コントロールAC検索
Gp.AC
•AC発行者
•ACシリアル番号
•所有者
•属性:
グループID
•属性値(グループID)
•対応グループID指定
コントロールAC-ID
応答
S353
グループ情報(コントロールAC)DBの例
発行者
グループID(サービスAC)
グループ情報(対応コントロールAC-1)
甲EE_SC
51001
定期点検 プロフェッショナル
51201
メンテナンスアイテムA
甲EE_SC
51001
定期点検 プロフェッショナル
51202
メンテナンスアイテムB
甲EE_SC
51001
定期点検 プロフェッショナル
51203
メンテナンスアイテムC
発行者
グループID(サービスAC)
グループ情報(対応コントロールAC-1)
甲EE_SC
51002
定期点検 エコノミー
51201
メンテナンスアイテムA
甲EE_SC
51002
定期点検 エコノミー
51204
メンテナンスアイテムD

Fig. 49

Fig.50

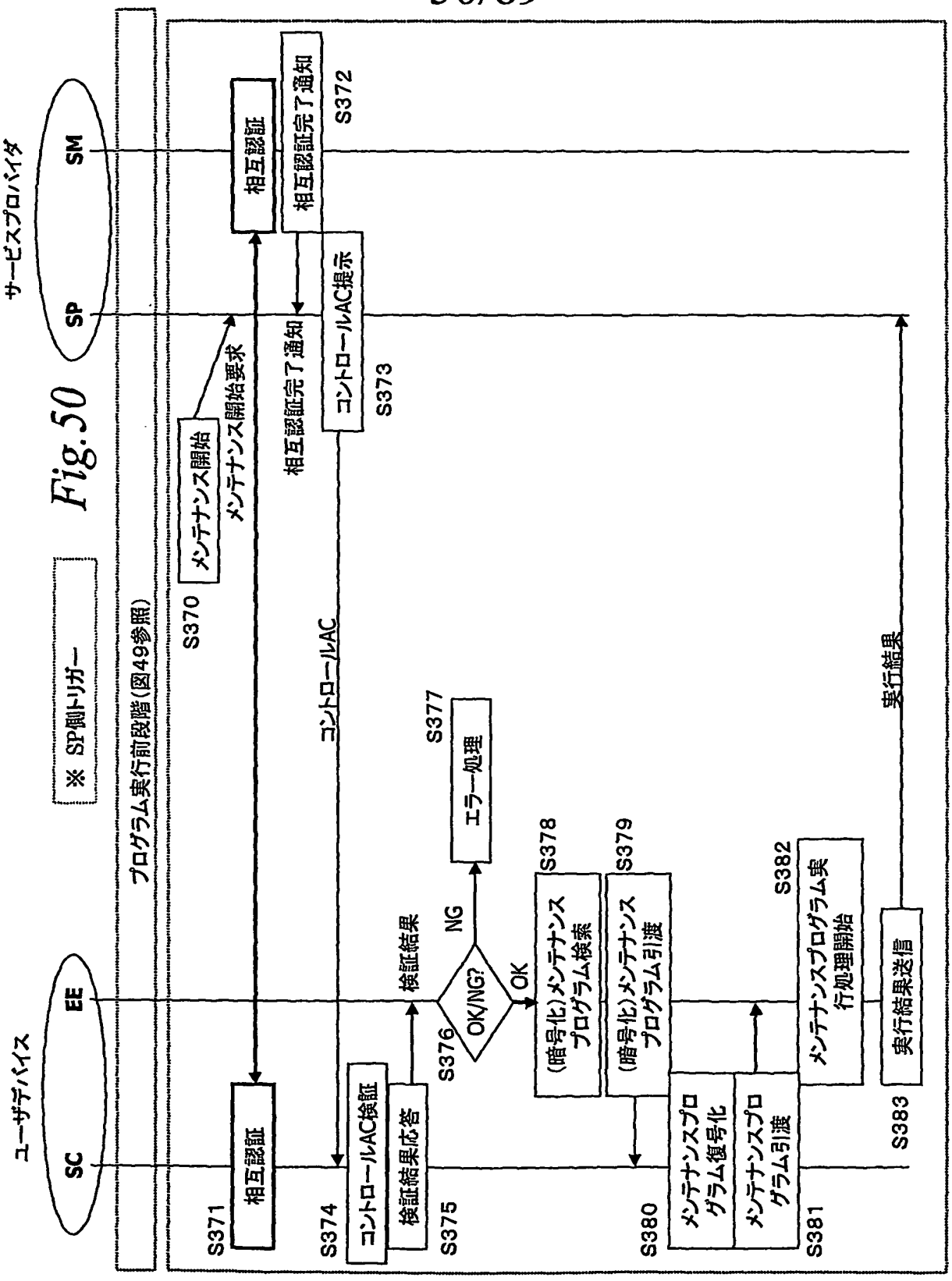

ユーザデバイス
SC
EE
サービスプロバイダ
SP
SM
※ SP側トリガー
プログラム実行前段階(図49参照)
S370
メンテナンス開始
メンテナンス開始要求
相互認証
S371
相互認証
相互認証完了通知
S372
コントロールAC提示
S373
コントロールAC
コントロールAC検証
S374
検証結果応答
検証結果
S375
OK/NG?
S376
NG
エラー処理
S377
OK
(暗号化)メンテナンスプログラム検索
S378
(暗号化)メンテナンスプログラム引渡
S379
メンテナンスプログラム復号化
S380
メンテナンスプログラム引渡
S381
メンテナンスプログラム実行処理開始
S382
実行結果送信
S383
実行結果

Fig.51

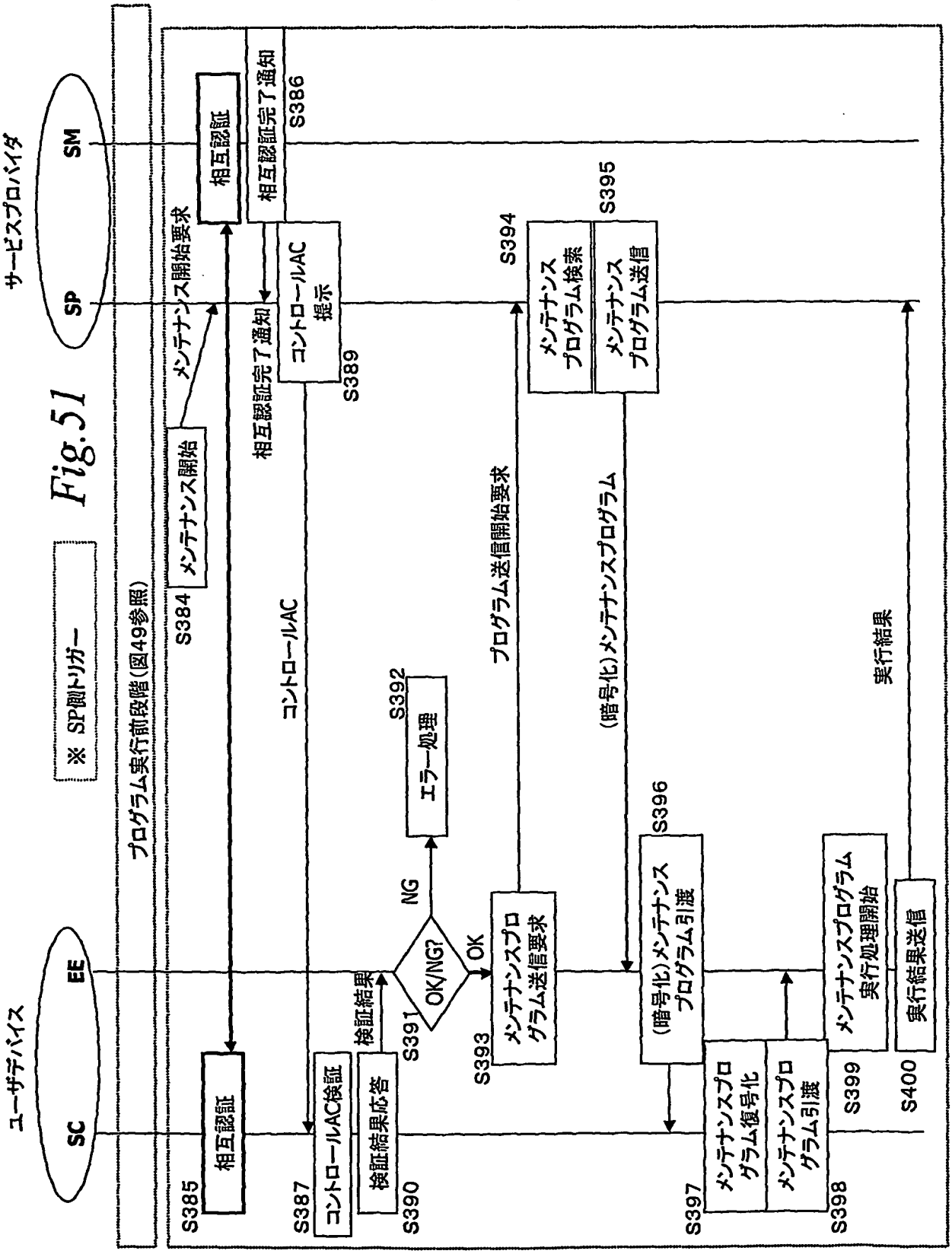
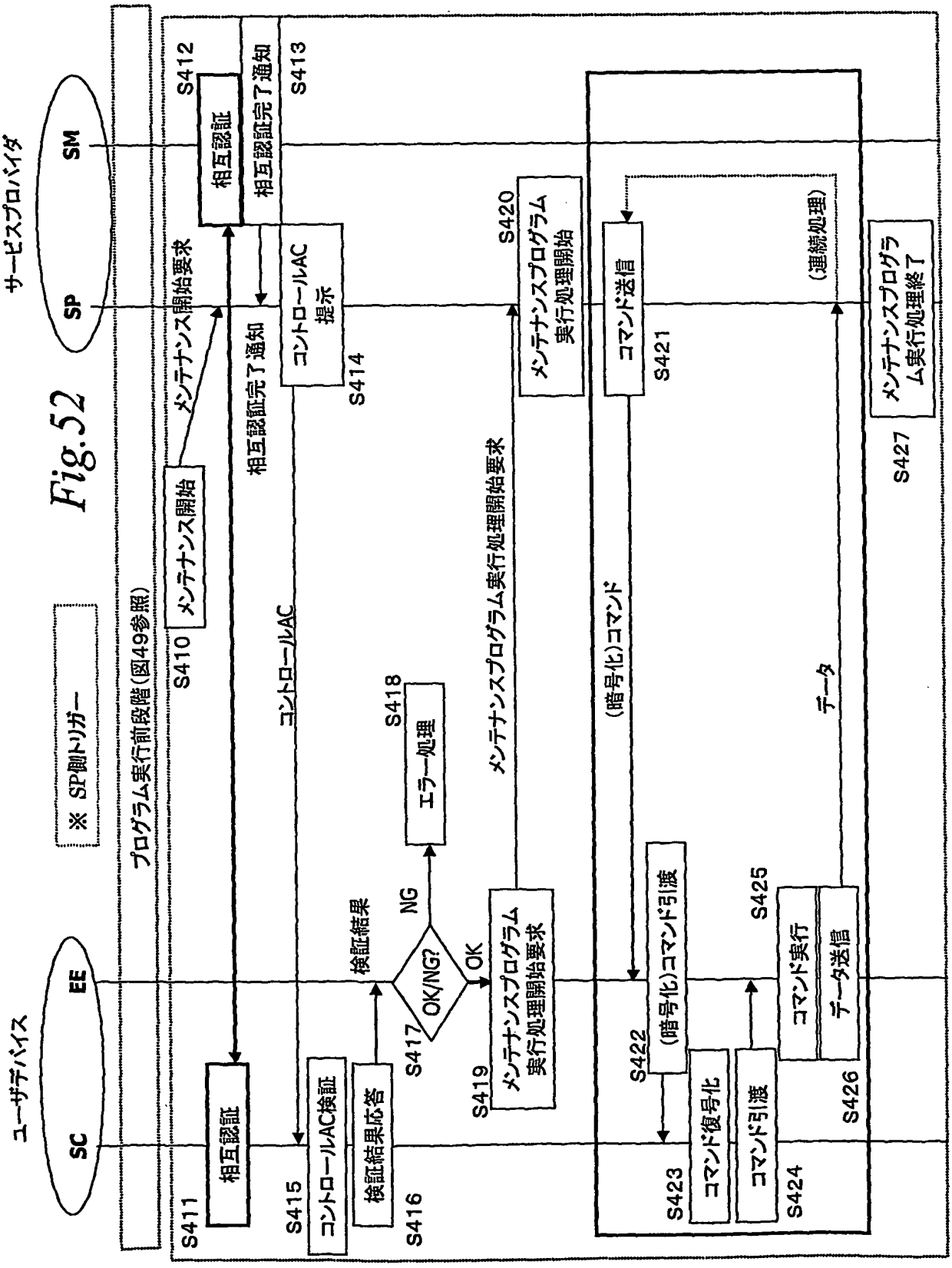

サービスプロバイダ
ユーザデバイス
SC
EE
SP
SM
※ SP側トリガー
プログラム実行前段階(図49参照)
S384 メンテナンス開始
メンテナンス開始要求
相互認証
相互認証完了通知
S386
コントロールAC
コントロールAC提示
S389
S385 相互認証
S387 コントロールAC検証
検証結果
検証結果応答
S390
S391 OK/NG?
NG
S392 エラー処理
OK
S393 メンテナンスプログラム送信要求
プログラム送信開始要求
S394 メンテナンスプログラム検索
S395 メンテナンスプログラム送信
(暗号化)メンテナンスプログラム
S396 (暗号化)メンテナンスプログラム引渡
S397 メンテナンスプログラム復号化
メンテナンスプログラム引渡
S398
S399 メンテナンスプログラム実行処理開始
実行結果
S400 実行結果送信

Fig.52


ユーザデバイス
サービスプロバイダ
SC
EE
SP
SM
※ SP側トリガー
プログラム実行前段階(図49参照)
S410 メンテナンス開始
メンテナンス開始要求
S411 相互認証
S412 相互認証
相互認証完了通知
S413 相互認証完了通知
S414 コントロールAC提示
コントロールAC
S415 コントロールAC検証
S416 検証結果応答
検証結果
S417 OK/NG?
NG
OK
S418 エラー処理
S419 メンテナンスプログラム実行処理開始要求
メンテナンスプログラム実行処理開始要求
S420 メンテナンスプログラム実行処理開始
S421 コマンド送信
(暗号化)コマンド
S422 (暗号化)コマンド引渡
S423 コマンド復号化
S424 コマンド引渡
S425 コマンド実行
S426 データ送信
データ
(連続処理)
S427 メンテナンスプログラム実行処理終了

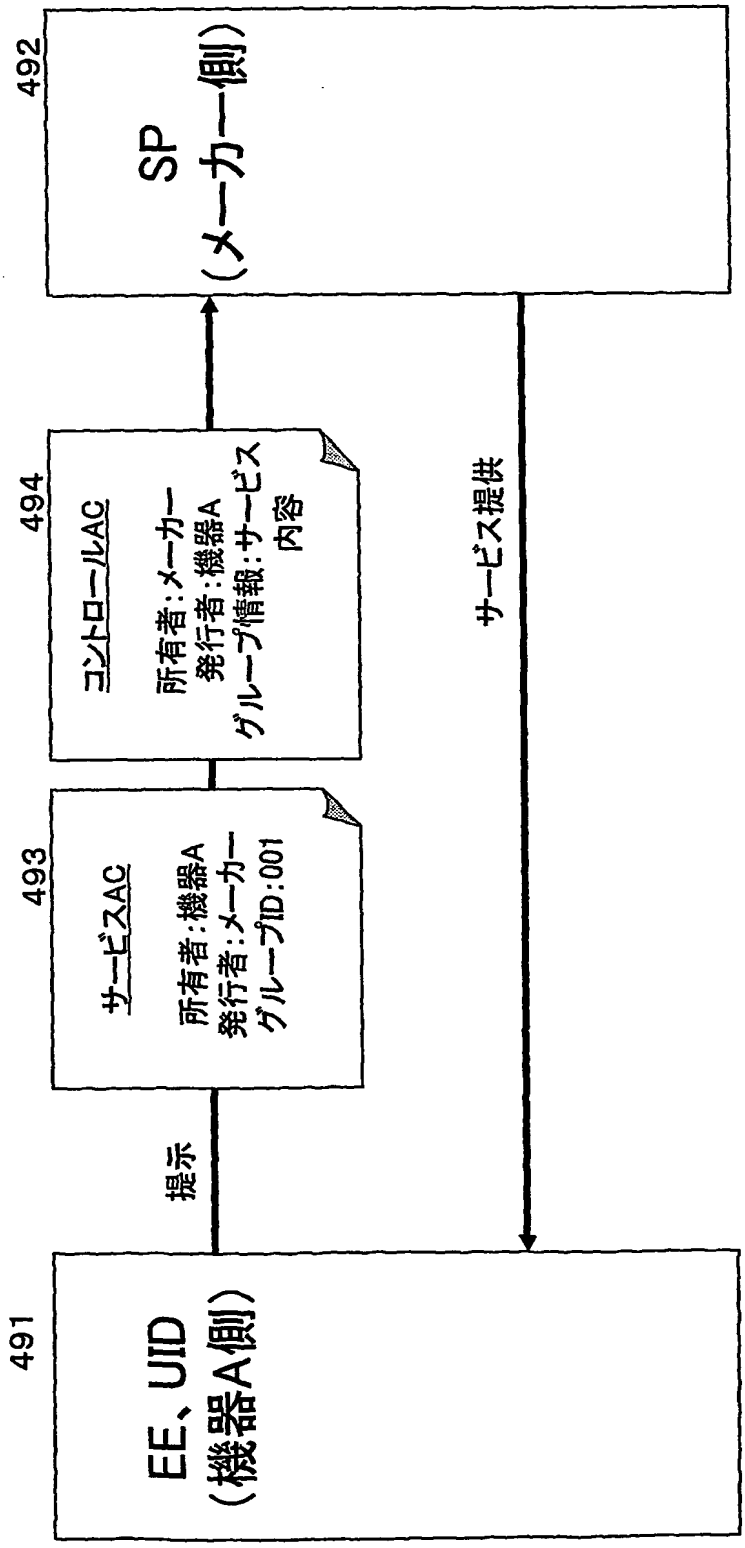

492
SP
(メーカー側)
494
ユントロールAC
所有者:メーカー
発行者:機器A
グループ情報:サービス内容
493
サービスAC
所有者:機器A
発行者:メーカー
グループID:001
提示
サービス提供
491
EE、UID
(機器A側)

Fig.53

	発行者	発行タイミング	所有者	検証者	属性
AC01	チャット 運営者(SP)	ログイン時	甲さん UID_USC or EE_SC	SP_SM	SP サーバアクセス権
AC02	Zさん(SP)	ログイン時	甲さん UID_USC or EE_SC	Zさん UID_USC or EE_SC	Z サーバアクセス権

Fig. 54

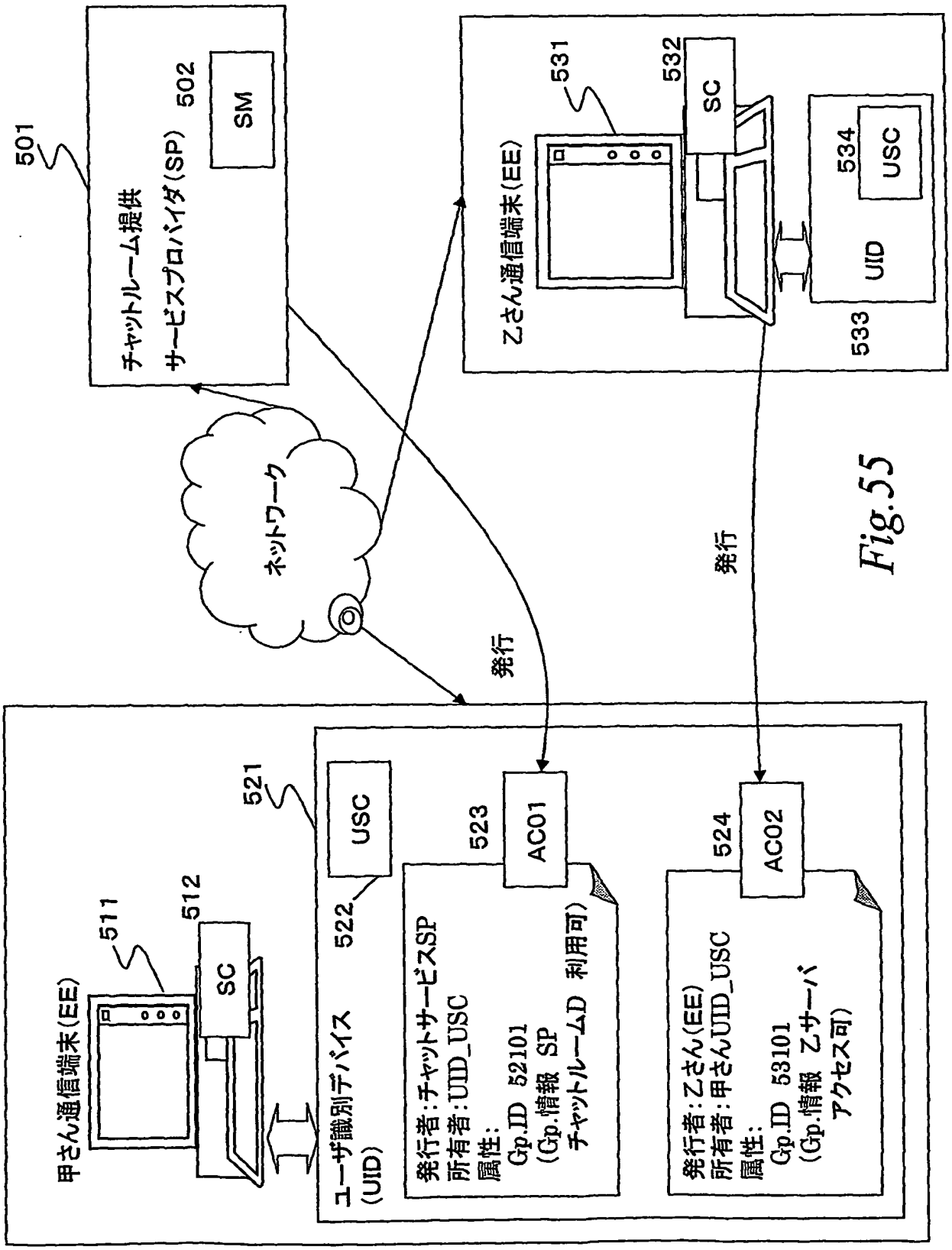

501
チャットルーム提供
サービスプロバイダ(SP)
502
SM
ネットワーク
Zさん通信端末(EE)
531
532
SC
534
USC
UID
533
発行
発行
甲さん通信端末(EE)
511
512
SC
521
USC
522
ユーザ識別デバイス
(UID)
523
AC01
発行者:チャットサービスSP
所有者:UID_USC
属性:
Gp.ID 52101
(Gp.情報 SP
チャットルームID 利用可)
524
AC02
発行者:Zさん(EE)
所有者:甲さんUID_USC
属性:
Gp.ID 53101
(Gp.情報 Zサーバ
アクセス可)

Fig.55

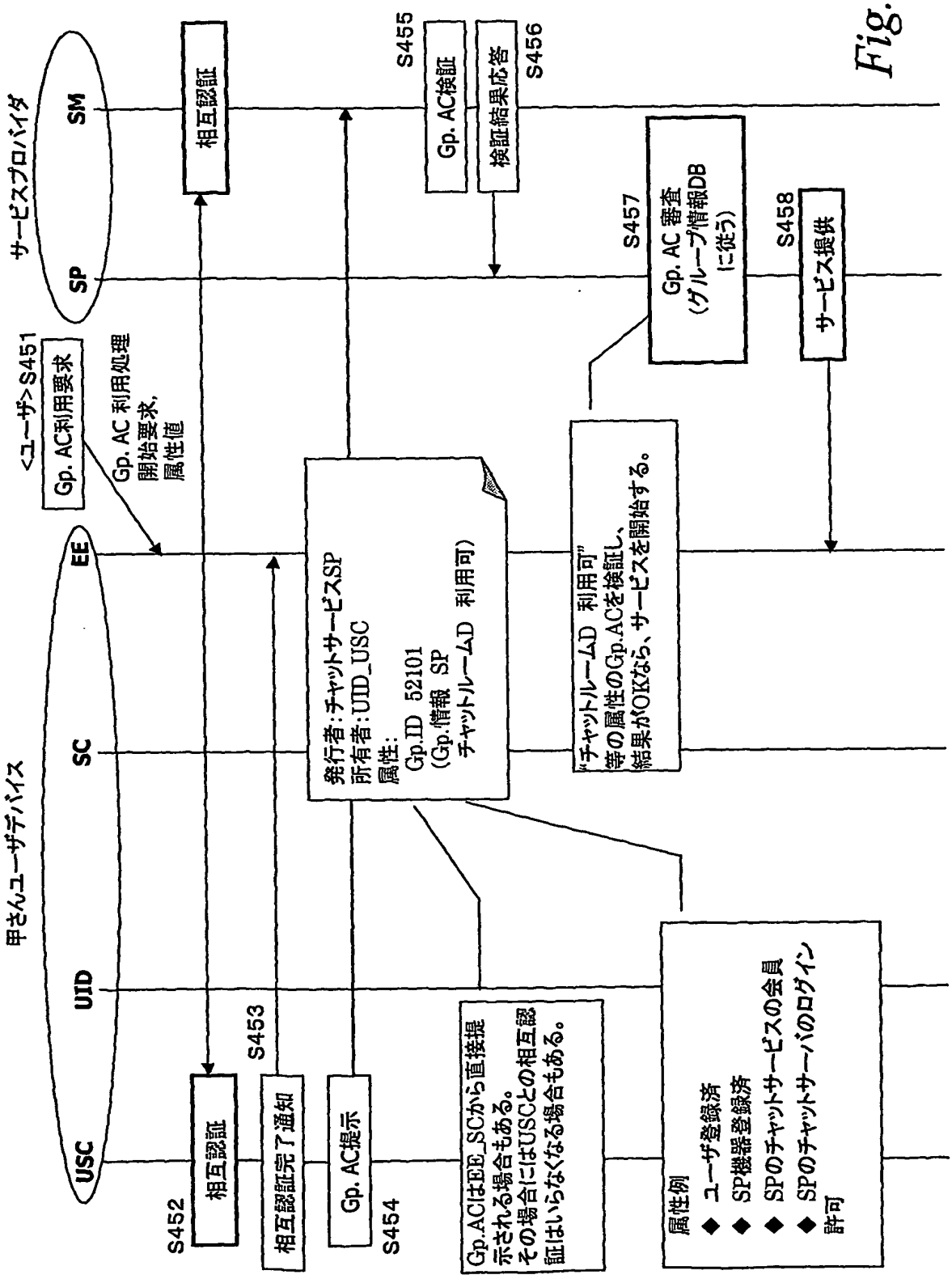

サービスプロバイダ
SM
SP
相互認証
S455
Gp. AC検証
検証結果応答
S456
S457
Gp. AC 審査
(グループ情報DB
に従う)
S458
サービス提供
<ユーザ>S451
Gp. AC利用要求
Gp. AC 利用処理
開始要求,
属性値
甲さんユーザデバイス
USC
UID
SC
EE
発行者:チャットサービスSP
所有者:UID_USC
属性:
Gp.ID 52101
(Gp.情報 SP
チャットルームID 利用可)
"チャットルームID 利用可"
等の属性のGp.ACを検証し、
結果がOKなら、サービスを開始する。
S453
S452
相互認証
相互認証完了通知
Gp. AC提示
S454
Gp.ACはEE_SCから直接提
示される場合もある。
その場合にはUSCとの相互認
証はいらなくなる場合もある。
属性例
◆ ユーザ登録済
◆ SP機器登録済
◆ SPのチャットサービスの会員
◆ SPのチャットサーバのログイン
許可

Fig.56

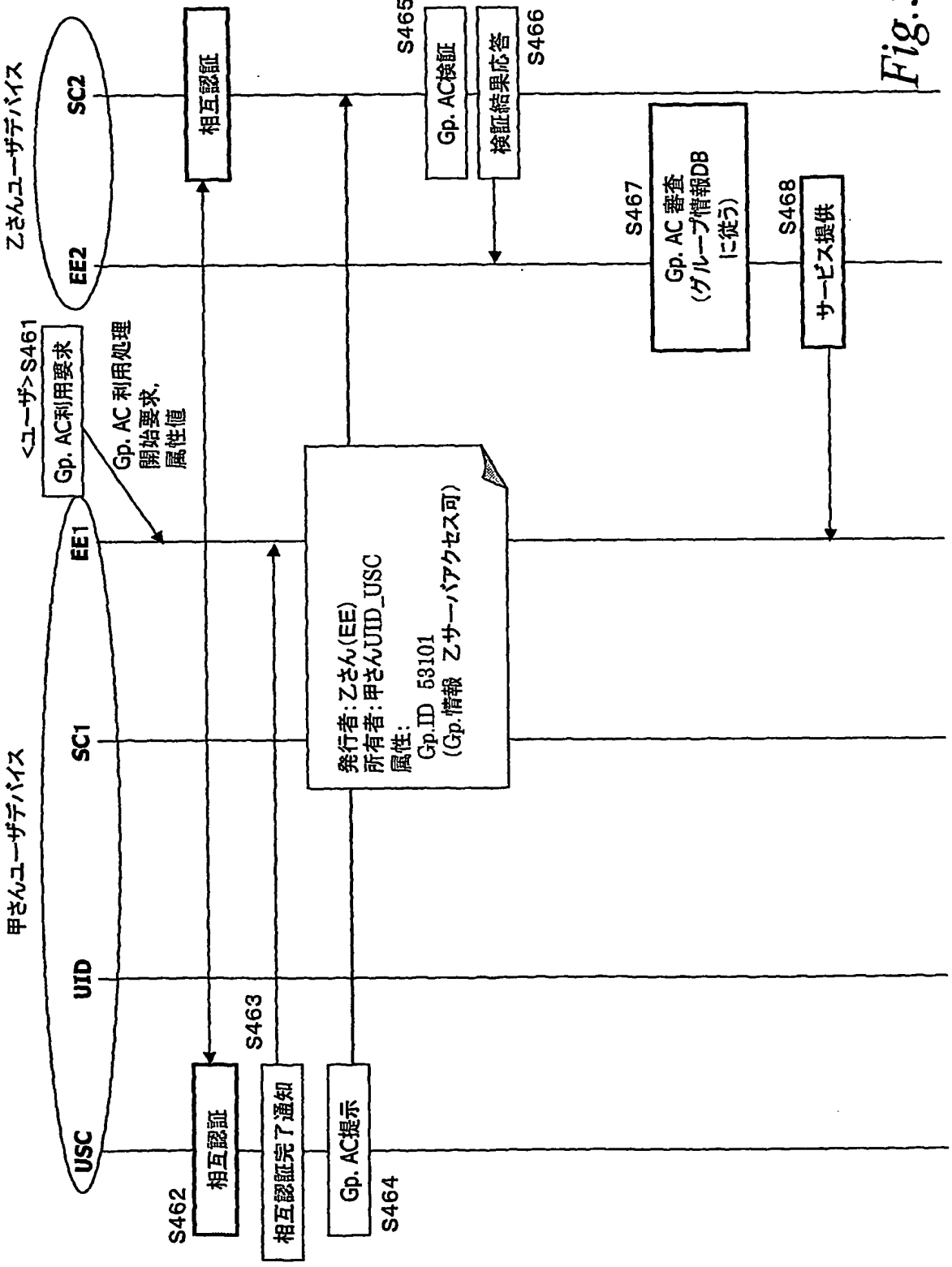

甲さんユーザデバイス
USC
UID
SC1
EE1
Zさんユーザデバイス
SC2
EE2
<ユーザ>S461
Gp. AC利用要求
Gp. AC 利用処理
開始要求,
属性値
相互認証
S462
相互認証
S463
相互認証完了通知
Gp. AC提示
S464
発行者:Zさん(EE)
所有者:甲さんUID_USC
属性:
Gp.ID 53101
(Gp.情報 Zサーバアクセス可)
S465
Gp. AC検証
S466
検証結果応答
S467
Gp. AC 審査
(グループ情報DB
に従う)
S468
サービス提供

Fig. 57

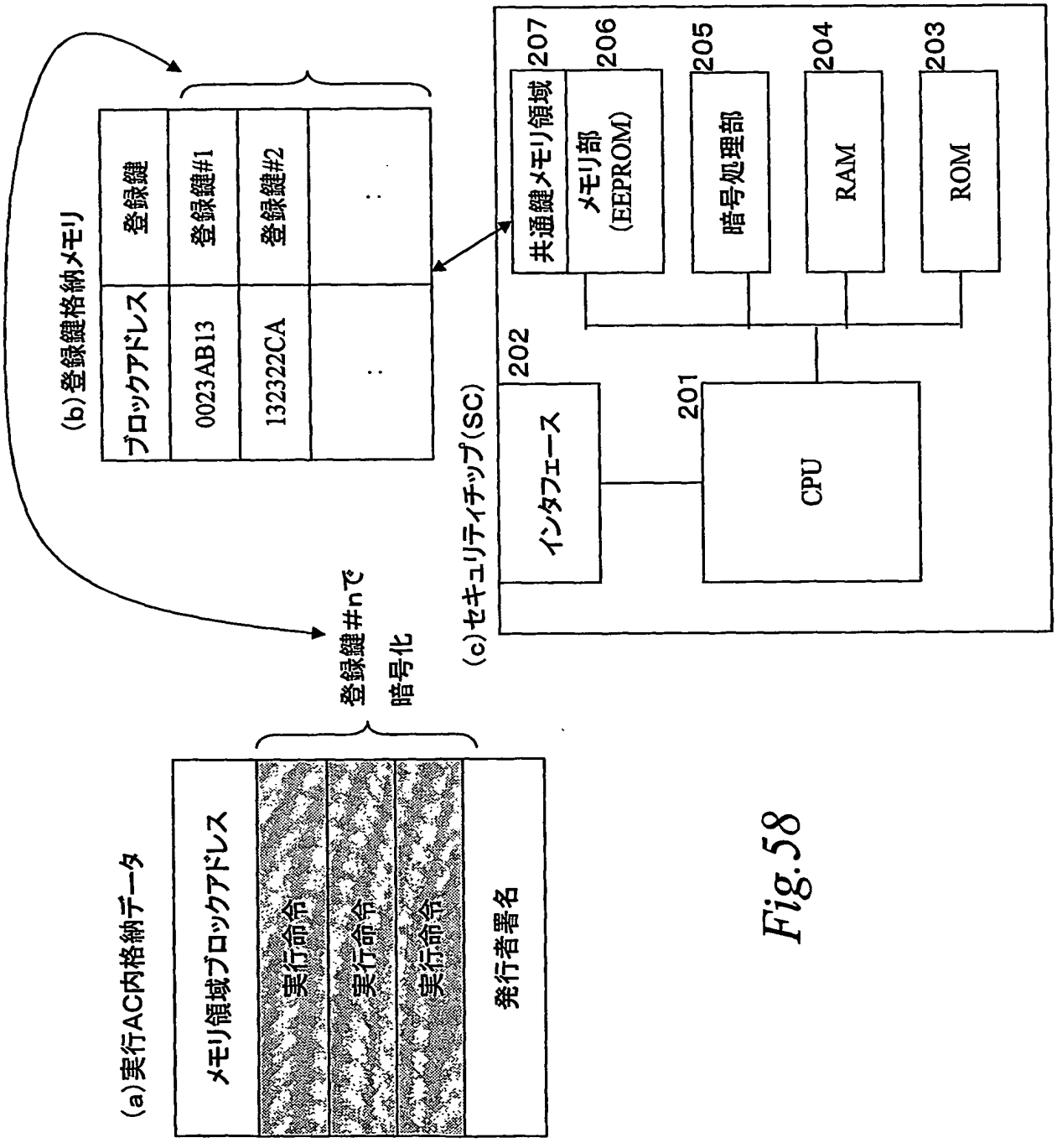
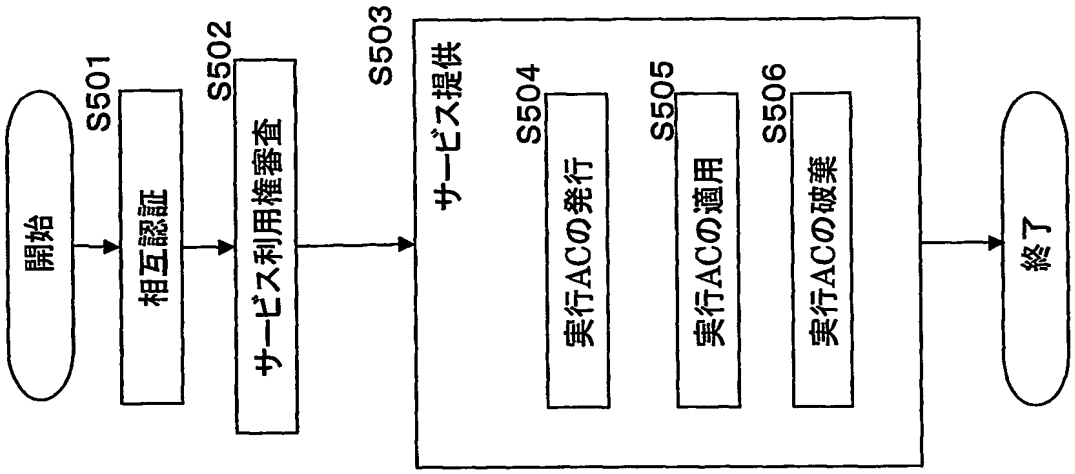

(a)実行AC内格納データ
メモリ領域ブロックアドレス
実行命令
実行命令
実行命令
発行者署名
登録鍵#nで
暗号化
(b)登録鍵格納メモリ
ブロックアドレス
登録鍵
0023AB13
登録鍵#1
132322CA
登録鍵#2
(c)セキュリティチップ(SC)
202
インタフェース
201
CPU
共通鍵メモリ領域
207
メモリ部
(EEPROM)
206
暗号処理部
205
RAM
204
ROM
203

Fig.58

Fig.59


開始
S501
相互認証
S502
サービス利用権審査
S503
サービス提供
S504
実行ACの発行
S505
実行ACの適用
S506
実行ACの破棄
終了

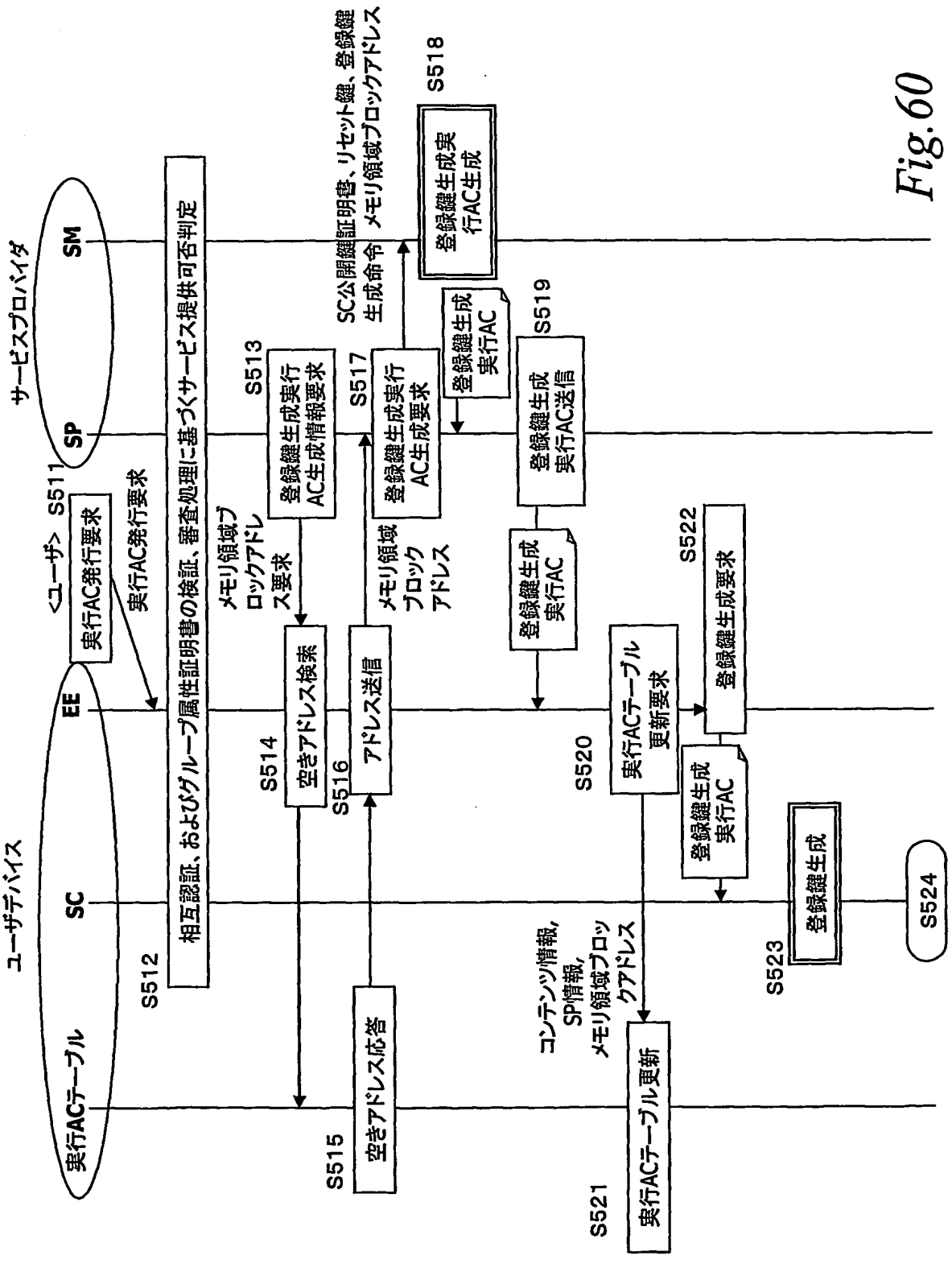

ユーザデバイス
サービスプロバイダ
EE
SC
SP
SM
実行ACテーブル
<ユーザ> S511
実行AC発行要求
実行AC発行要求
S512
相互認証、およびグループ属性証明書の検証、審査処理に基づくサービス提供可否判定
S513
登録鍵生成実行AC生成情報要求
メモリ領域ブロックアドレス要求
S514
空きアドレス検索
S515
空きアドレス応答
S516
アドレス送信
メモリ領域ブロックアドレス
S517
登録鍵生成実行AC生成要求
SC公開鍵証明書、リセット鍵、登録鍵生成命令
メモリ領域ブロックアドレス
S518
登録鍵生成実行AC生成
登録鍵生成実行AC
S519
登録鍵生成実行AC送信
登録鍵生成実行AC
S520
コンテンツ情報、SP情報、メモリ領域ブロックアドレス
実行ACテーブル更新
S521
実行ACテーブル更新要求
S522
登録鍵生成要求
登録鍵生成実行AC
S523
登録鍵生成
S524

Fig.60

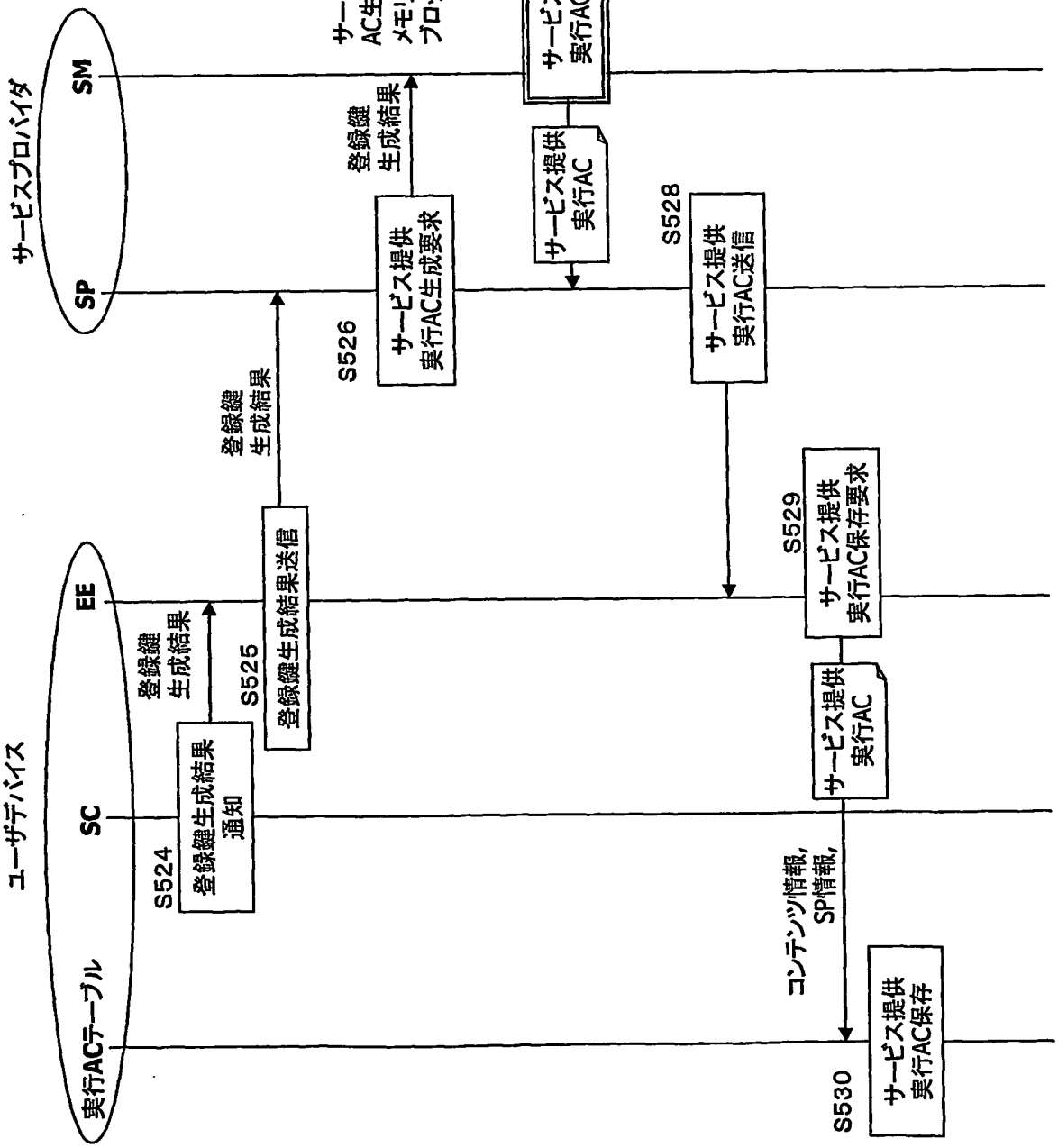
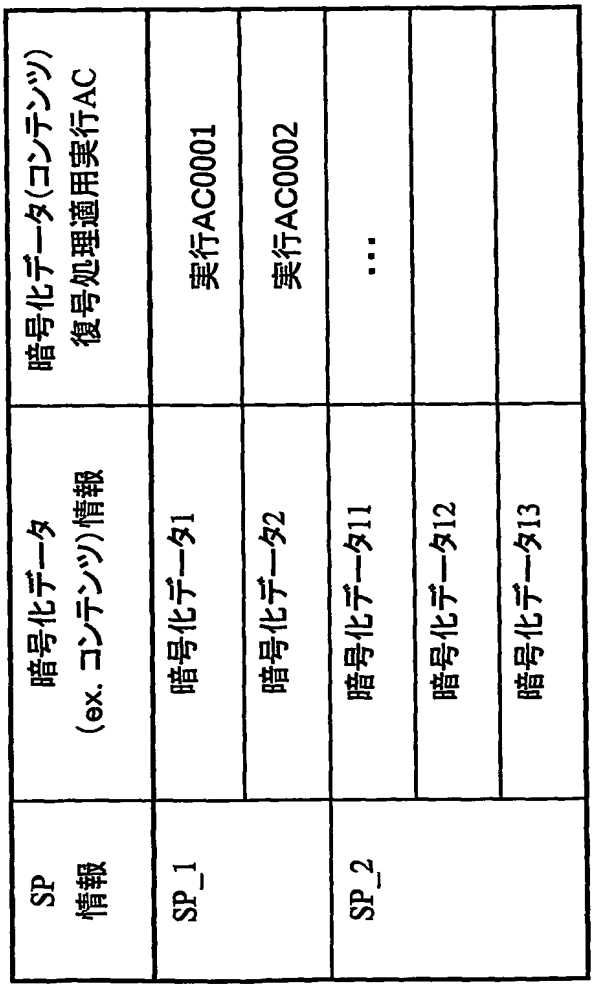

ユーザデバイス
実行ACテーブル
EE
SC
サービスプロバイダ
SP
SM
S524
登録鍵生成結果通知
登録鍵
生成結果
S525
登録鍵生成結果送信
登録鍵
生成結果
S526
サービス提供
実行AC生成要求
サービス提供実行
AC生成要求,
メモリ領域
ブロックアドレス,
S527
サービス提供
実行AC生成
サービス提供
実行AC
S528
サービス提供
実行AC送信
S529
サービス提供
実行AC保存要求
サービス提供
実行AC
コンテンツ情報,
SP情報,
S530
サービス提供
実行AC保存

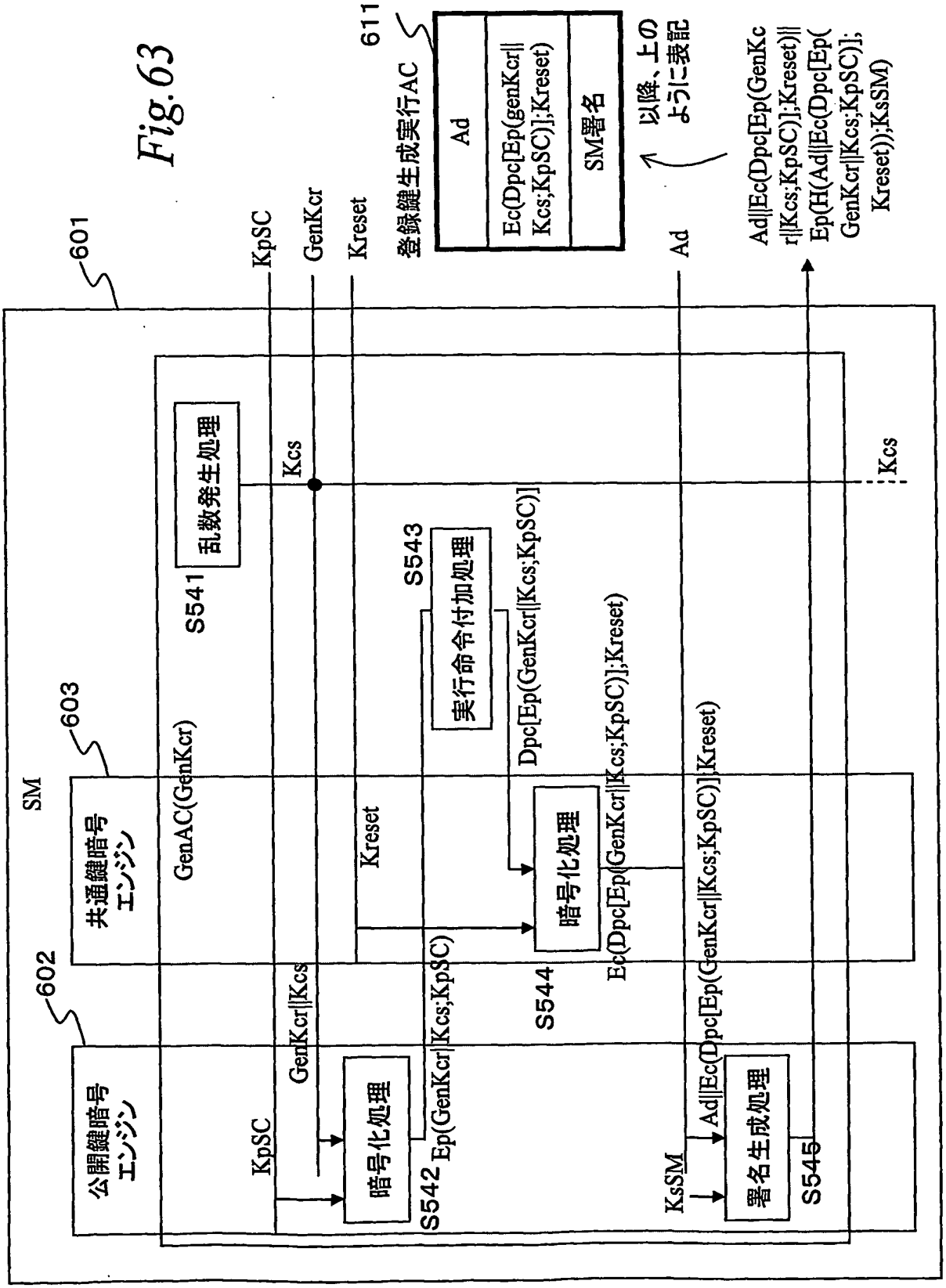
Fig.61



SP 情報	暗号化データ (ex. コンテンツ)情報	暗号化データ(コンテンツ) 復号処理適用実行AC
SP_1	暗号化データ1	実行AC0001
	暗号化データ2	実行AC0002
SP_2	暗号化データ11	...
	暗号化データ12	
	暗号化データ13	

Fig.62

Fig.63


SM
601
602
603
611
公開鍵暗号エンジン
共通鍵暗号エンジン
GenAC(GenKcr)
乱数発生処理
S541
暗号化処理
S542
Ep(GenKcr||Kcs;KpSC)
実行命令付加処理
S543
暗号化処理
S544
Ec(Dpc[Ep(GenKcr||Kcs;KpSC)];Kreset)
署名生成処理
S545
KpSC
GenKcr||Kcs
Kreset
Kcs
Dpc[Ep(GenKcr||Kcs;KpSC)]
Ad||Ec(Dpc[Ep(GenKcr||Kcs;KpSC)];Kreset)
KsSM
登録鍵生成実行AC
Ad
Ec(Dpc[Ep(genKcr||Kcs;KpSC)];Kreset)
SM署名
以降、上のように表記
Ad||Ec(Dpc[Ep(GenKcr||Kcs;KpSC)];Kreset)||Ep(H(Ad||Ec(Dpc[Ep(GenKcr||Kcs;KpSC)];Kreset));KsSM)

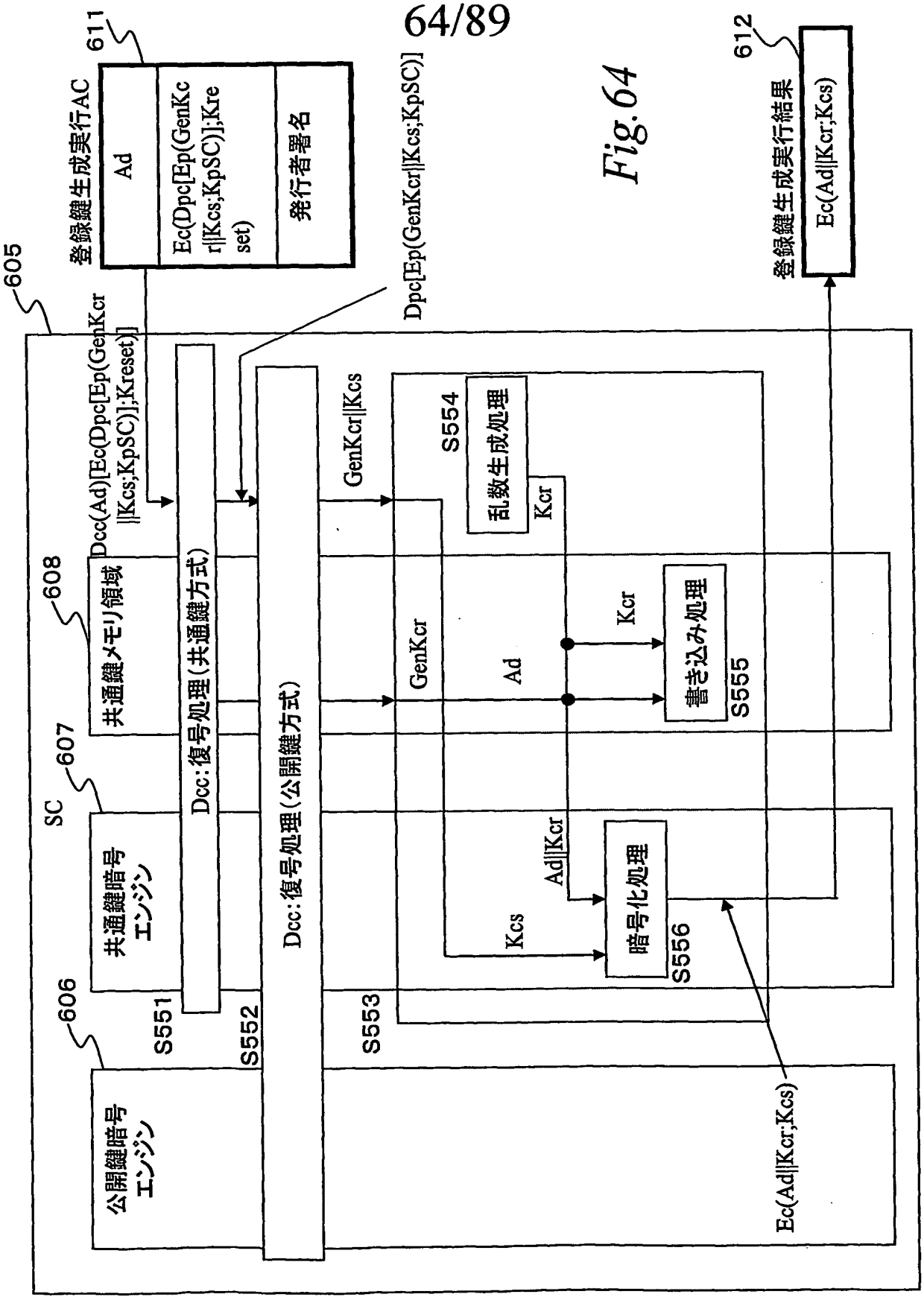
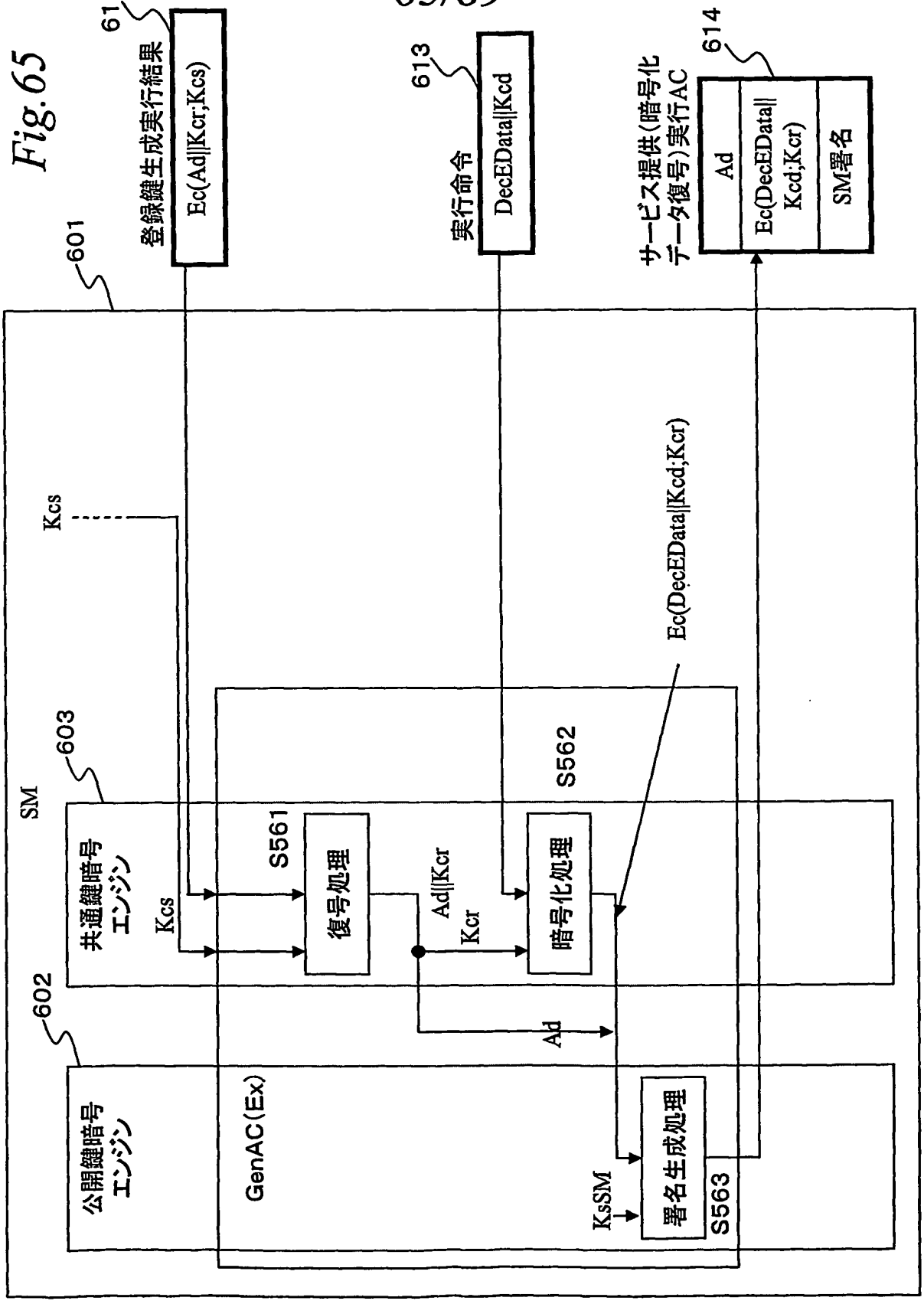

605
SC
606
公開鍵暗号エンジン
607
共通鍵暗号エンジン
608
共通鍵メモリ領域
611
登録鍵生成実行AC
Ad
Ec(Dpc[Ep(GenKcr||Kcs;KpSC)];Kreset)
発行者署名
612
登録鍵生成実行結果
Ec(Ad||Kcr;Kcs)
Dcc(Ad)[Ec(Dpc[Ep(GenKcr||Kcs;KpSC)];Kreset)]
Dpc[Ep(GenKcr||Kcs;KpSC)]
Dcc:復号処理(共通鍵方式)
Dcc:復号処理(公開鍵方式)
GenKcr||Kcs
S551
S552
S553
S554
乱数生成処理
Kcr
GenKcr
Ad
Kcr
書き込み処理
S555
Ad||Kcr
Kcs
暗号化処理
S556
Ec(Ad||Kcr;Kcs)

Fig. 64

Fig. 65


612
登録鍵生成実行結果
Ec(Ad||Kcr;Kcs)
613
実行命令
DecEData||Kcd
614
サービス提供(暗号化データ復号)実行AC
Ad
Ec(DecEData||Kcd;Kcr)
SM署名
601
Kcs
Ec(DecEData||Kcd;Kcr)
603
SM
共通鍵暗号エンジン
Kcs
S561
復号処理
Ad||Kcr
Kcr
S562
暗号化処理
602
公開鍵暗号エンジン
GenAC(Ex)
Ad
KsSM
署名生成処理
S563

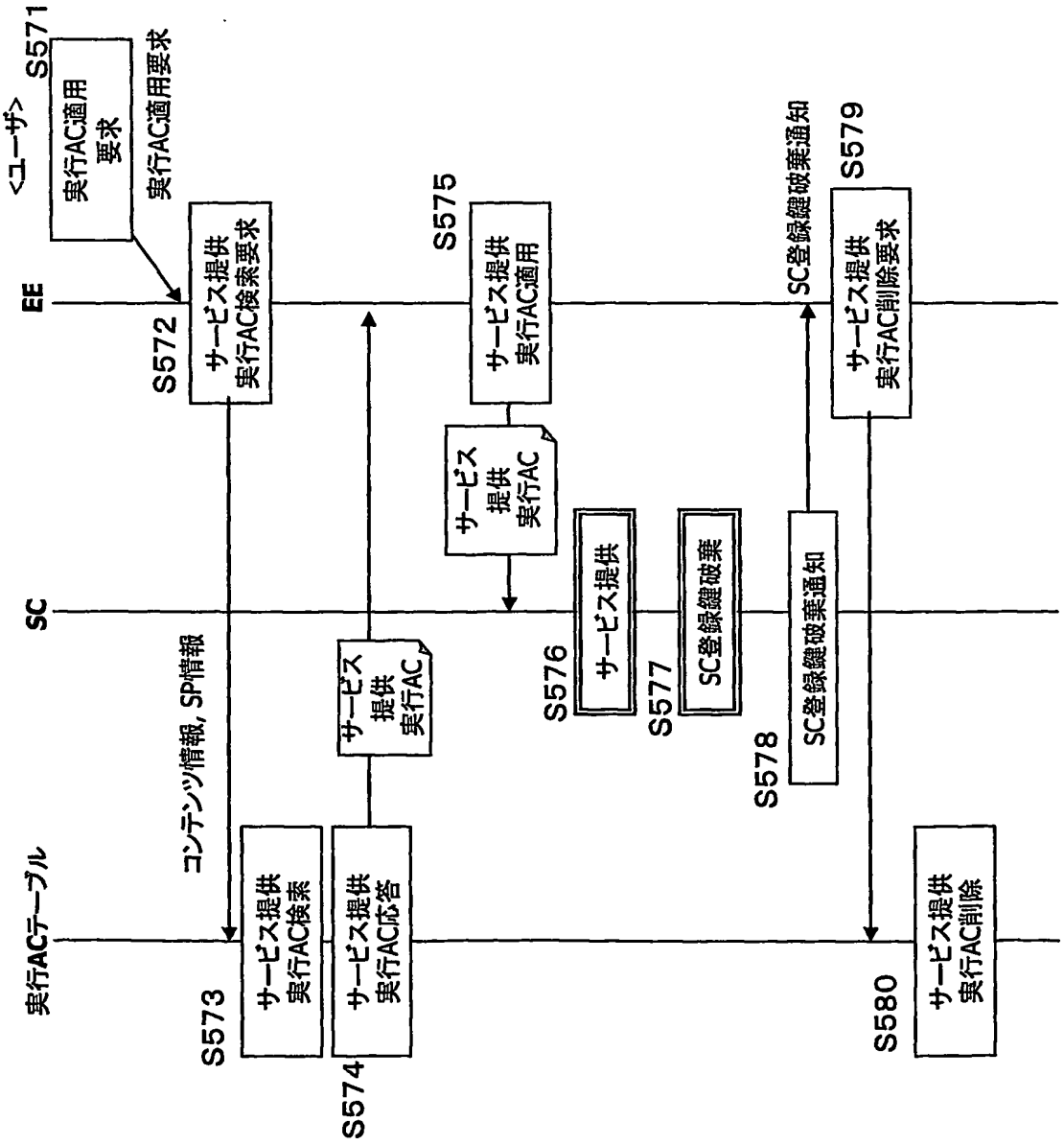

<ユーザ>
S571
実行AC適用要求
実行AC適用要求
EE
S572
サービス提供実行AC検索要求
S575
サービス提供実行AC適用
SC登録鍵破棄通知
S579
サービス提供実行AC削除要求
サービス提供実行AC
SC
サービス提供実行AC
S576
サービス提供
S577
SC登録鍵破棄
S578
SC登録鍵破棄通知
コンテンツ情報, SP情報
実行ACテーブル
S573
サービス提供実行AC検索
S574
サービス提供実行AC応答
S580
サービス提供実行AC削除

Fig.66

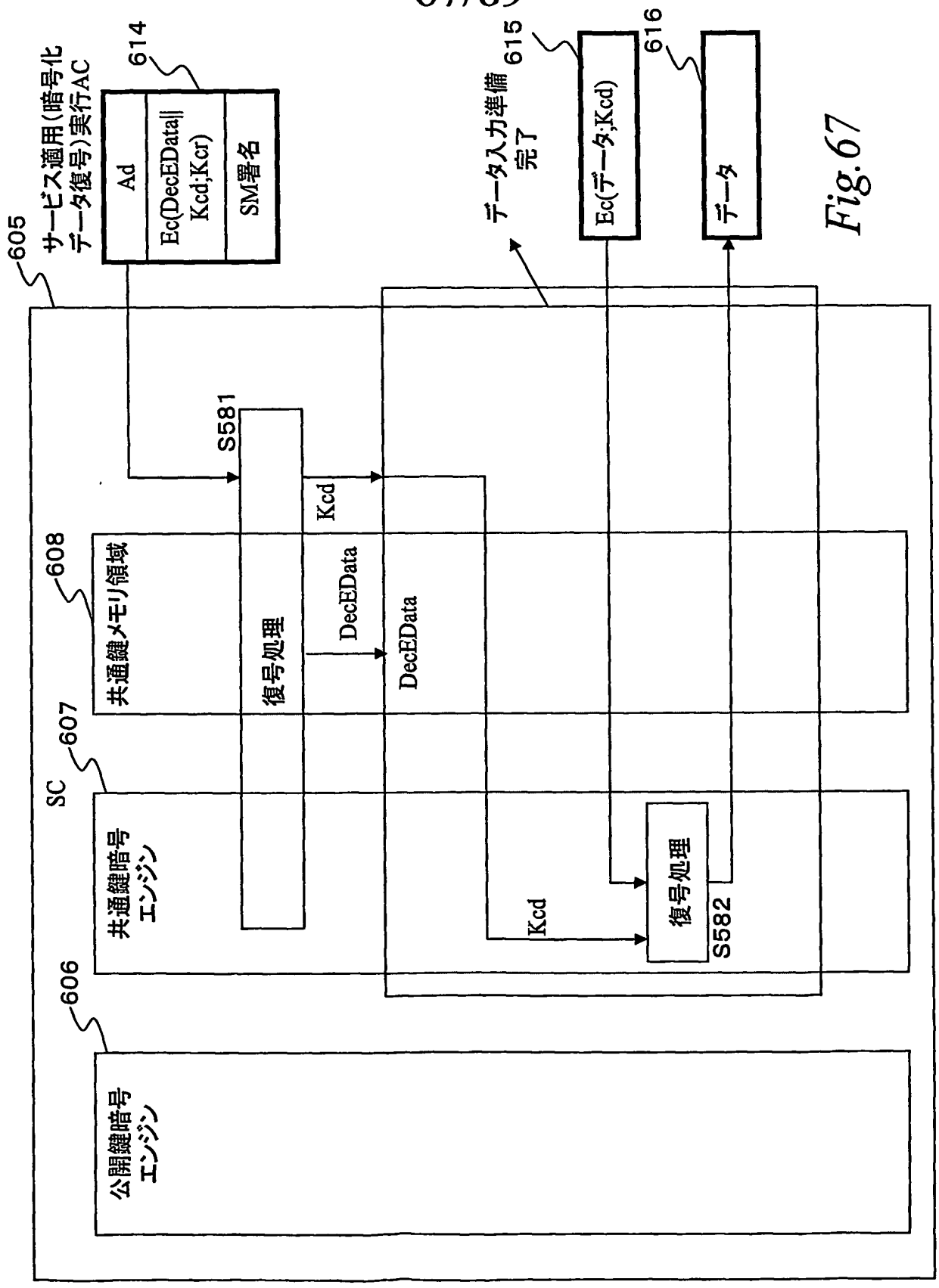

605
サービス適用(暗号化データ復号)実行AC
614
Ad
Ec(DecEData||Kcd;Kcr)
SM署名
データ入力準備完了
615
Ec(データ;Kcd)
616
データ
S581
Kcd
608
共通鍵メモリ領域
復号処理
DecEData
DecEData
SC
607
共通鍵暗号エンジン
Kcd
復号処理
S582
606
公開鍵暗号エンジン

Fig.67

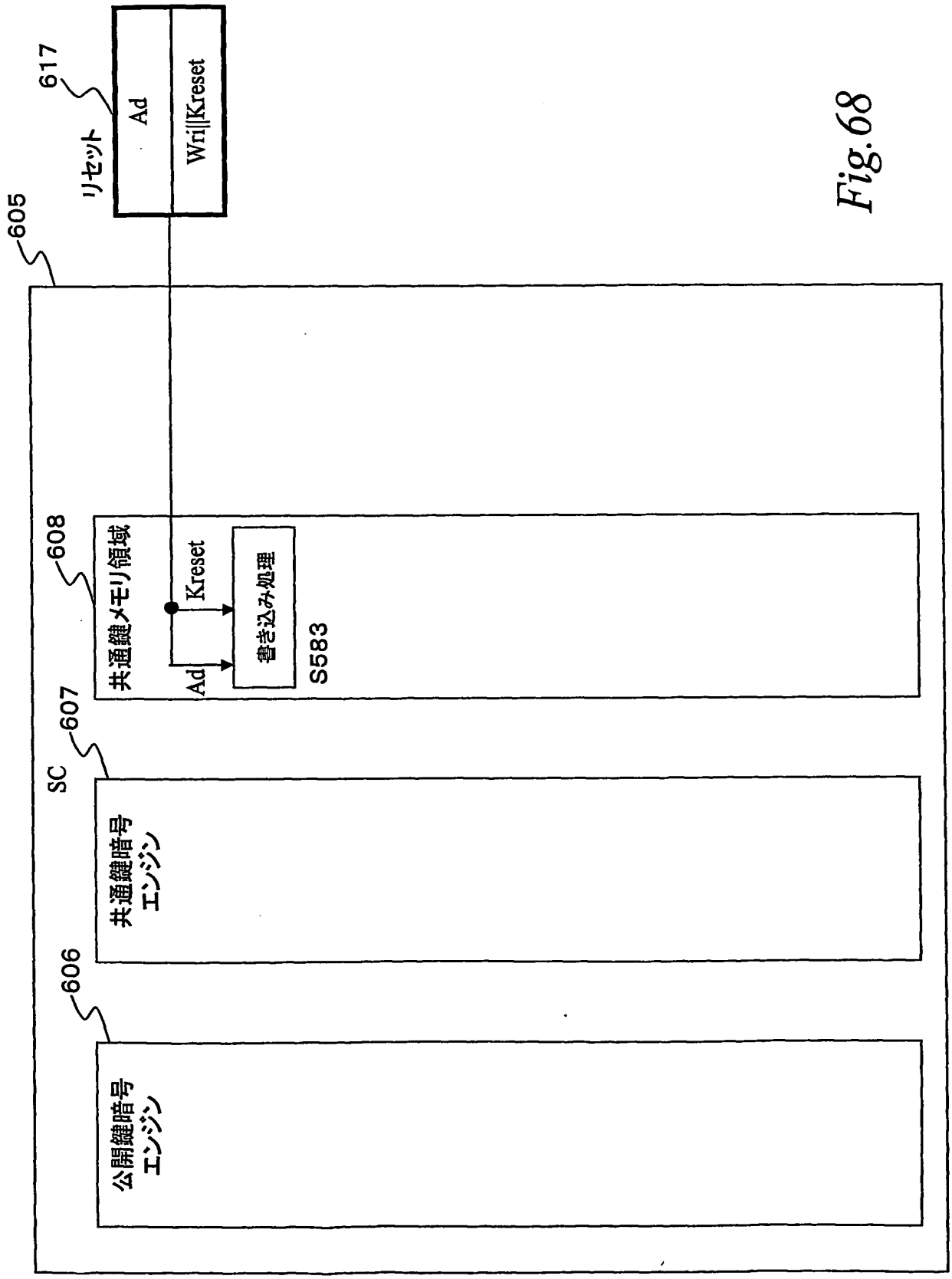

617
リセット
Ad
Wri||Kreset
605
608
共通鍵メモリ領域
Kreset
Ad
書き込み処理
S583
SC
607
共通鍵暗号
エンジン
606
公開鍵暗号
エンジン

Fig.68

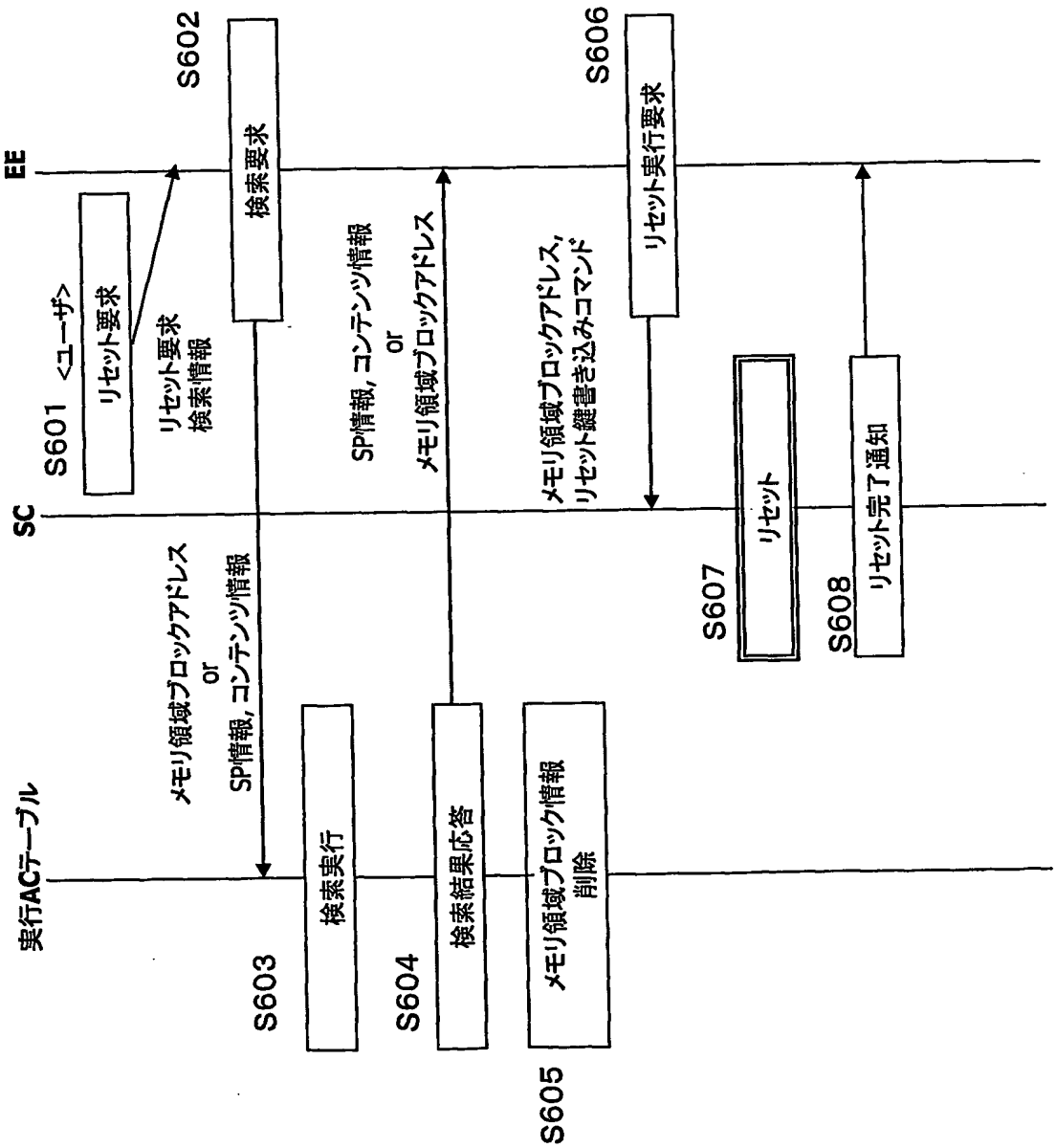

EE
SC
実行ACテーブル
S601 <ユーザ>
リセット要求
リセット要求
検索情報
S602
検索要求
メモリ領域ブロックアドレス
or
SP情報, コンテンツ情報
S603
検索実行
SP情報, コンテンツ情報
or
メモリ領域ブロックアドレス
S604
検索結果応答
メモリ領域ブロック情報
削除
S605
メモリ領域ブロックアドレス,
リセット鍵書き込みコマンド
S606
リセット実行要求
S607
リセット
S608
リセット完了通知

Fig.69

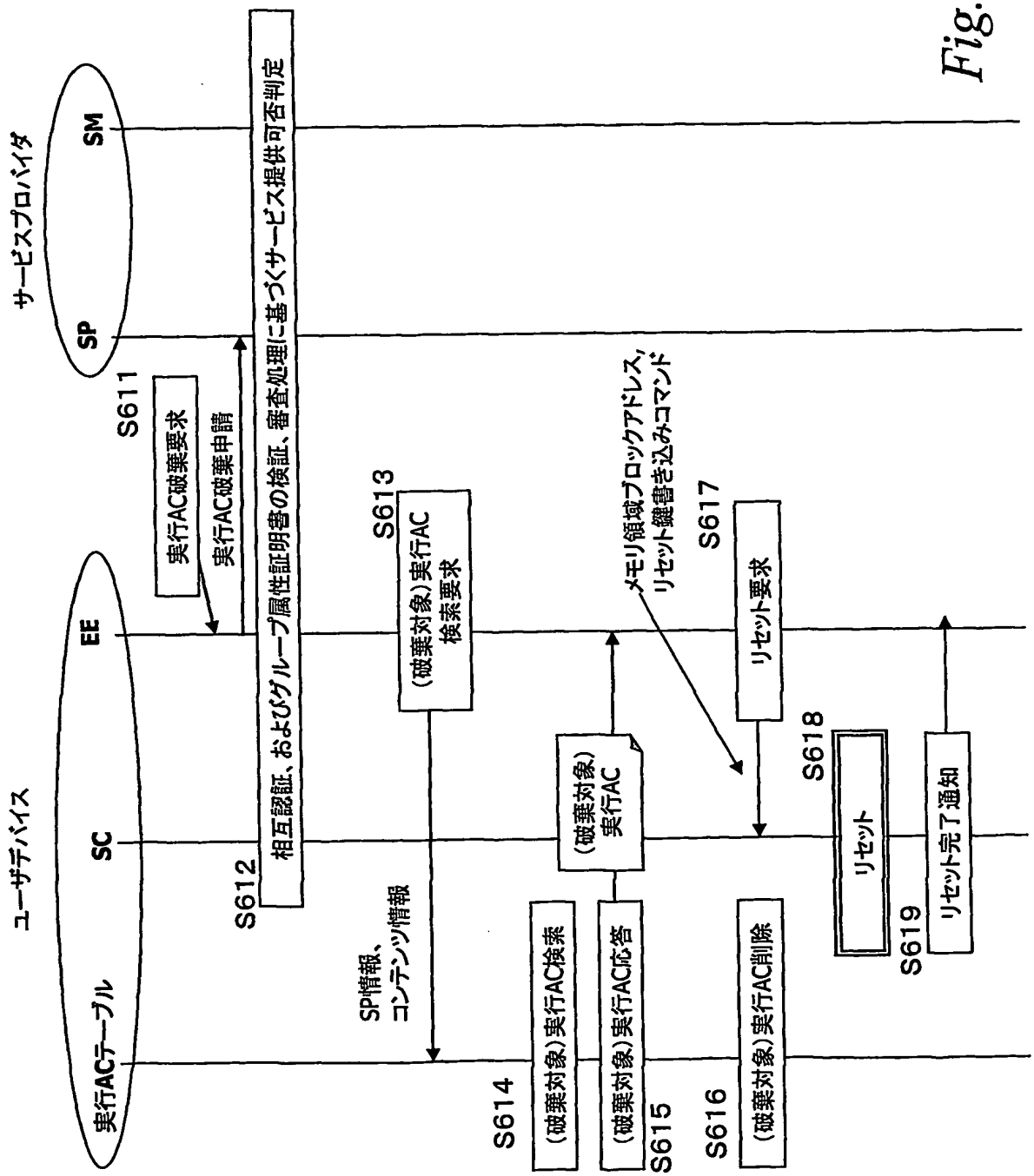

ユーザデバイス
サービスプロバイダ
EE
SC
SP
SM
実行ACテーブル
S611
実行AC破棄要求
実行AC破棄申請
S612
相互認証、およびグループ属性証明書の検証、審査処理に基づくサービス提供可否判定
S613
(破棄対象)実行AC検索要求
SP情報、コンテンツ情報
S614
(破棄対象)実行AC検索
(破棄対象)実行AC
メモリ領域ブロックアドレス、リセット鍵書き込みコマンド
S615
(破棄対象)実行AC応答
S616
(破棄対象)実行AC削除
S617
リセット要求
S618
リセット
S619
リセット完了通知

Fig. 70

Fig. 71

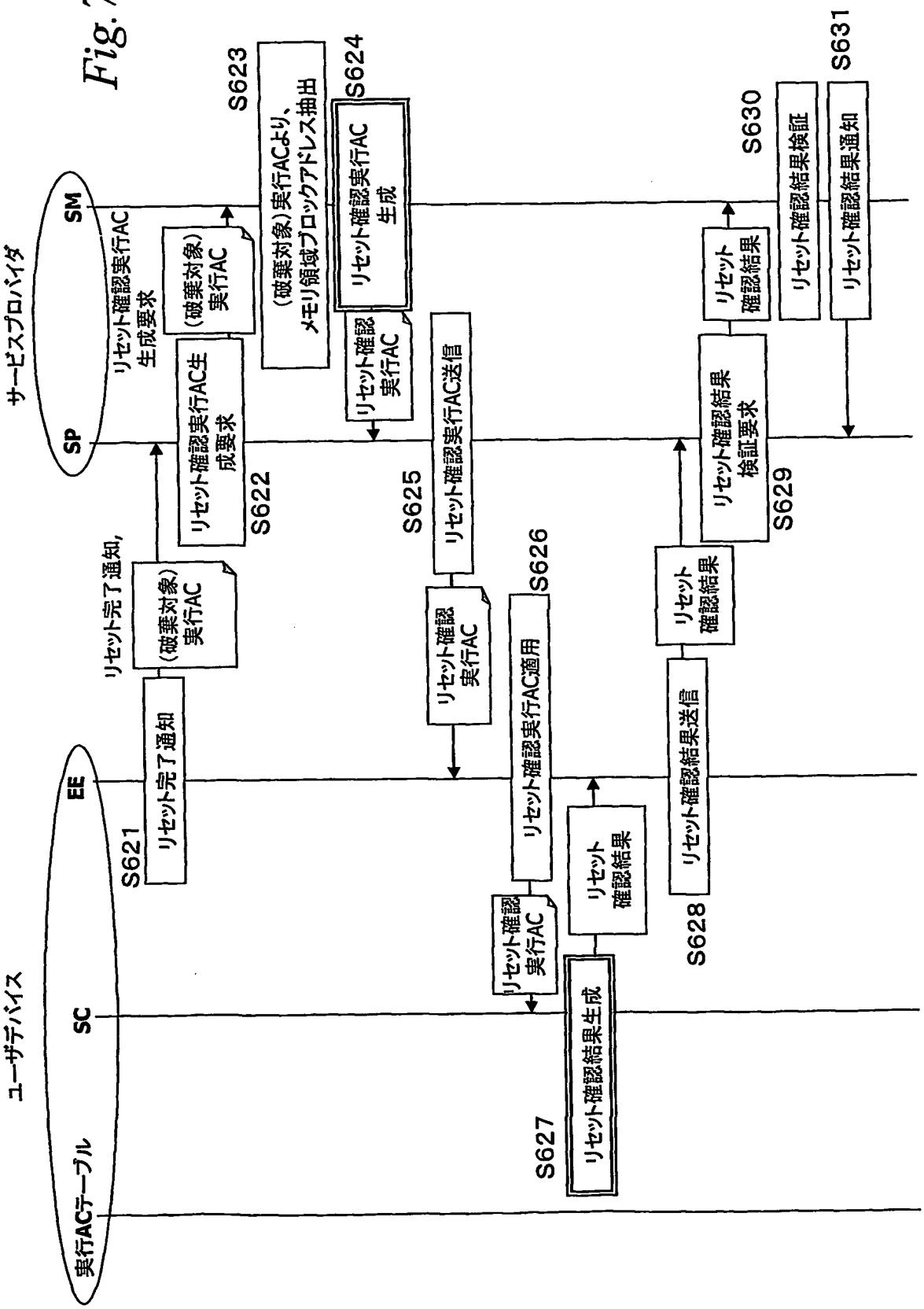
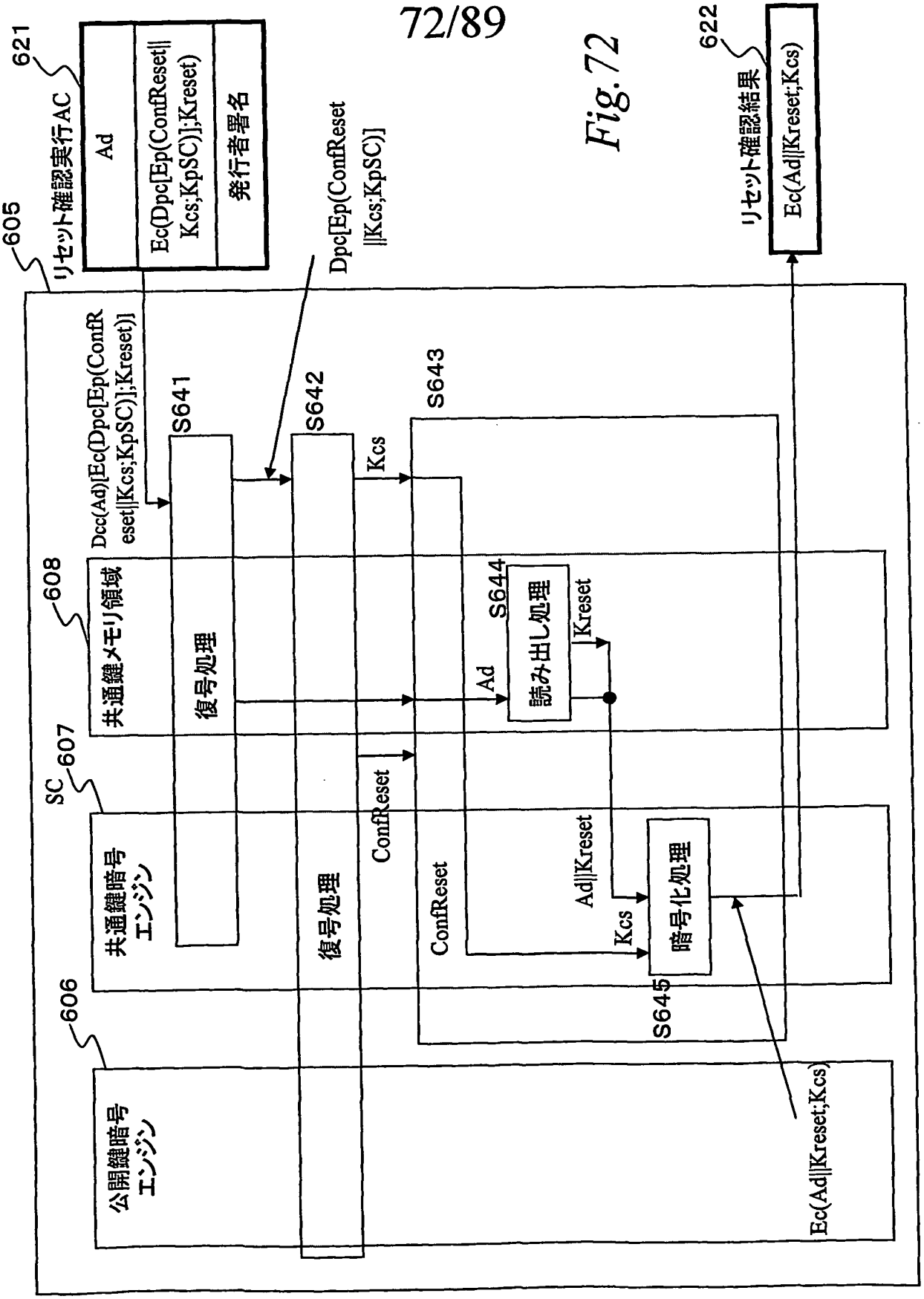

サービスプロバイダ
SM
SP
ユーザデバイス
EE
SC
実行ACテーブル
リセット確認実行AC生成要求
(破棄対象)実行AC
リセット確認実行AC生成要求
S622
(破棄対象)実行AC
(破棄対象)実行ACより、メモリ領域ブロックアドレス抽出
S623
リセット確認実行AC生成
S624
リセット確認実行AC
リセット確認実行AC送信
S625
リセット確認実行AC適用
S626
リセット確認結果生成
S627
リセット確認結果送信
S628
リセット確認結果検証
S629
リセット確認結果通知
S630
S631
リセット確認結果
リセット確認実行AC
リセット確認結果
リセット確認実行AC
リセット確認結果
リセット完了通知
S621
(破棄対象)実行AC
リセット完了通知,

Fig. 72


605
リセット確認実行AC
621
Ad
Ec(Dpc[Ep(ConfReset||Kcs;KpSC)];Kreset)
発行者署名
622
リセット確認結果
Ec(Ad||Kreset;Kcs)
Dpc[Ep(ConfReset||Kcs;KpSC)]
Dcc(Ad)[Ec(Dpc[Ep(ConfReset||Kcs;KpSC)];Kreset)]
S641
S642
S643
S644
S645
608
共通鍵メモリ領域
復号処理
SC
607
共通鍵暗号エンジン
606
公開鍵暗号エンジン
復号処理
Kcs
ConfReset
ConfReset
Ad
読み出し処理
Kreset
Ad||Kreset
Kcs
暗号化処理
Ec(Ad||Kreset;Kcs)

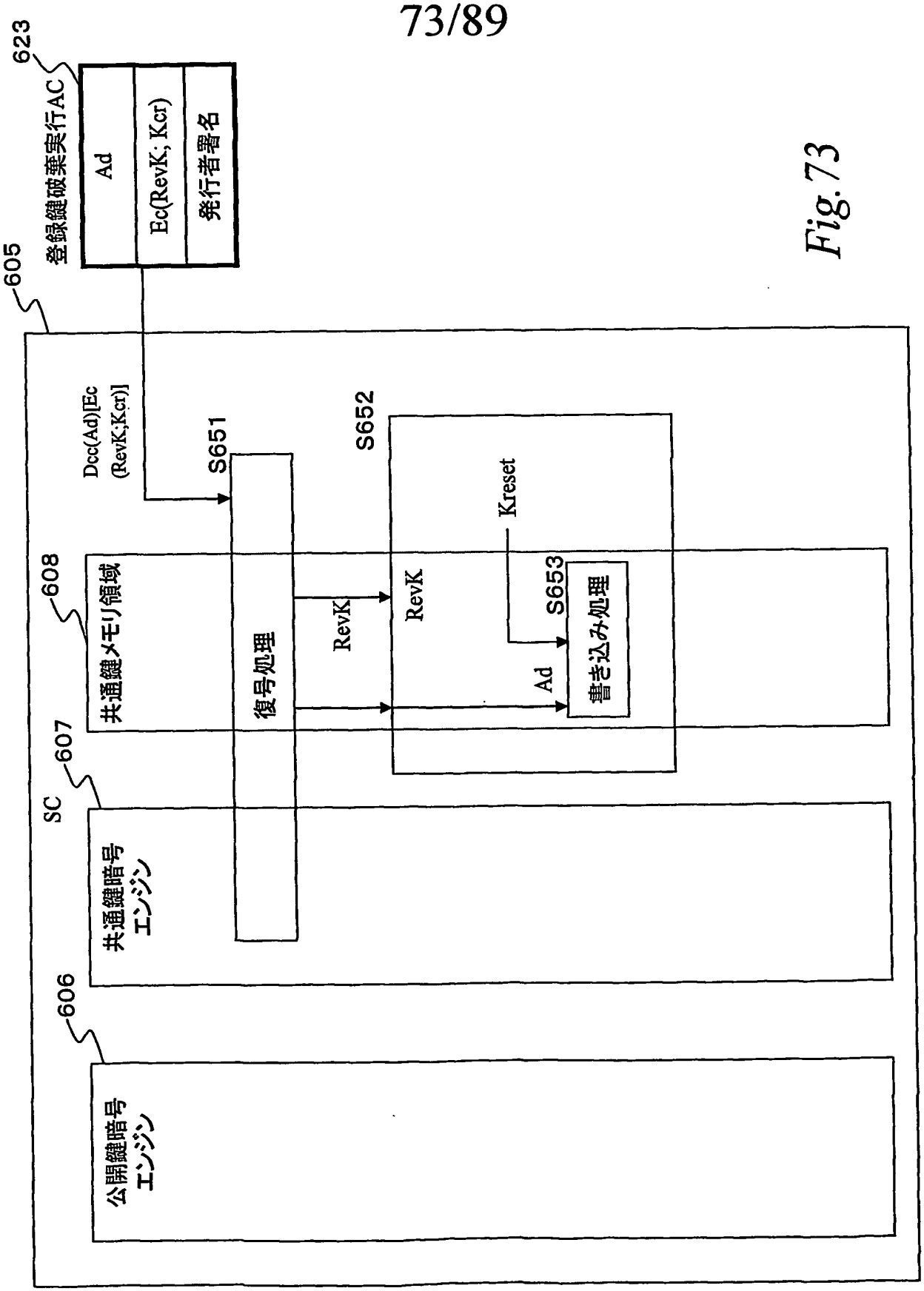

623
登録鍵破棄実行AC
Ad
Ec(RevK; Kcr)
発行者署名
605
Dcc(Ad)[Ec (RevK;Kcr)]
S651
S652
608
共通鍵メモリ領域
復号処理
RevK
RevK
Kreset
S653
Ad
書き込み処理
607
SC
共通鍵暗号 エンジン
606
公開鍵暗号 エンジン

Fig. 73

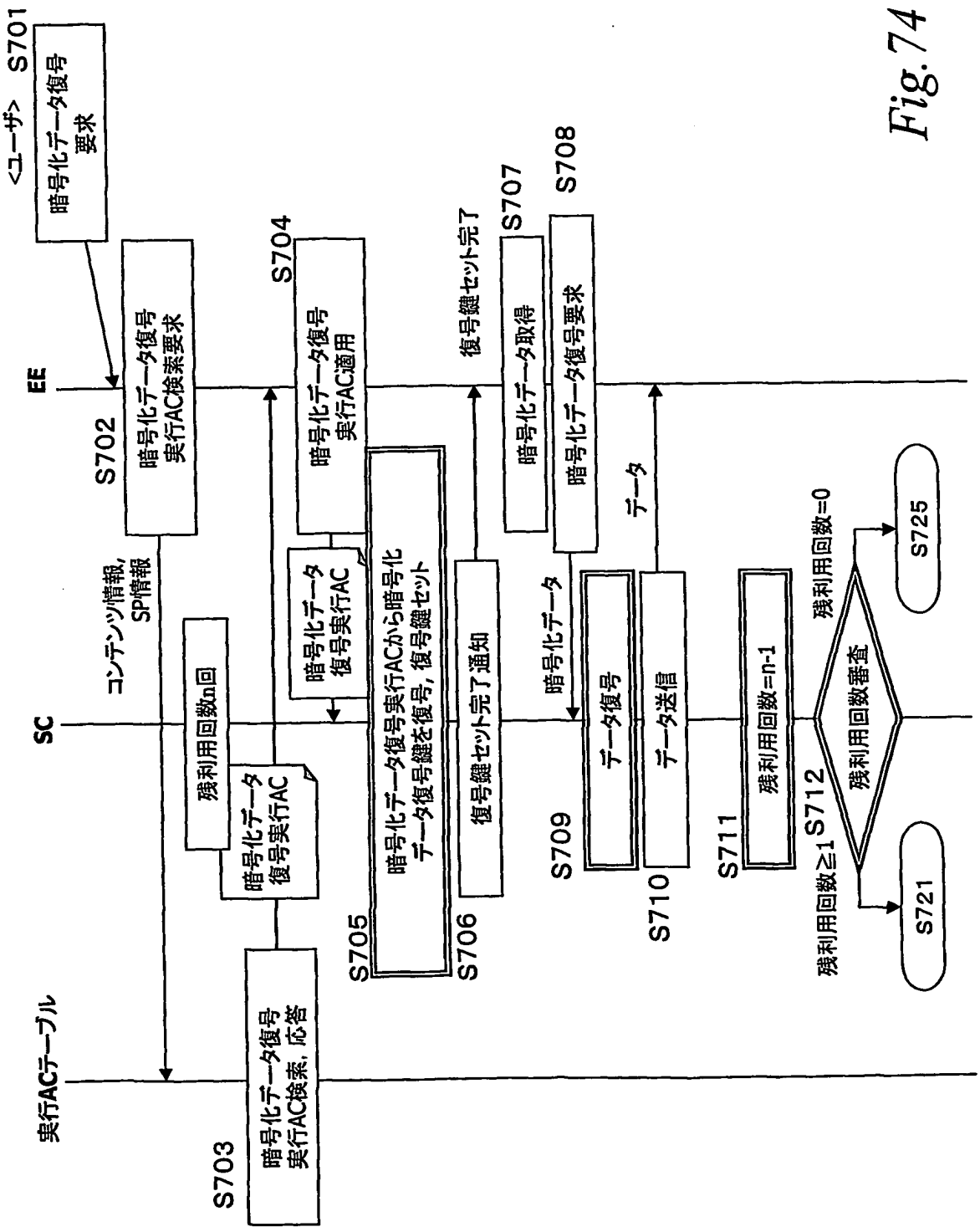

<ユーザ>
S701
暗号化データ復号要求
EE
S702
暗号化データ復号実行AC検索要求
S704
暗号化データ復号実行AC適用
S707
暗号化データ取得
S708
暗号化データ復号要求
復号鍵セット完了
コンテンツ情報, SP情報
SC
残利用回数n回
暗号化データ復号実行AC
暗号化データ復号実行ACから暗号化データ復号鍵を復号, 復号鍵セット
S705
S706
復号鍵セット完了通知
暗号化データ
S709
データ復号
データ
S710
データ送信
S711
残利用回数=n-1
S712
残利用回数審査
残利用回数=0
S725
残利用回数≧1
S721
実行ACテーブル
S703
暗号化データ復号実行AC検索, 応答

Fig. 74

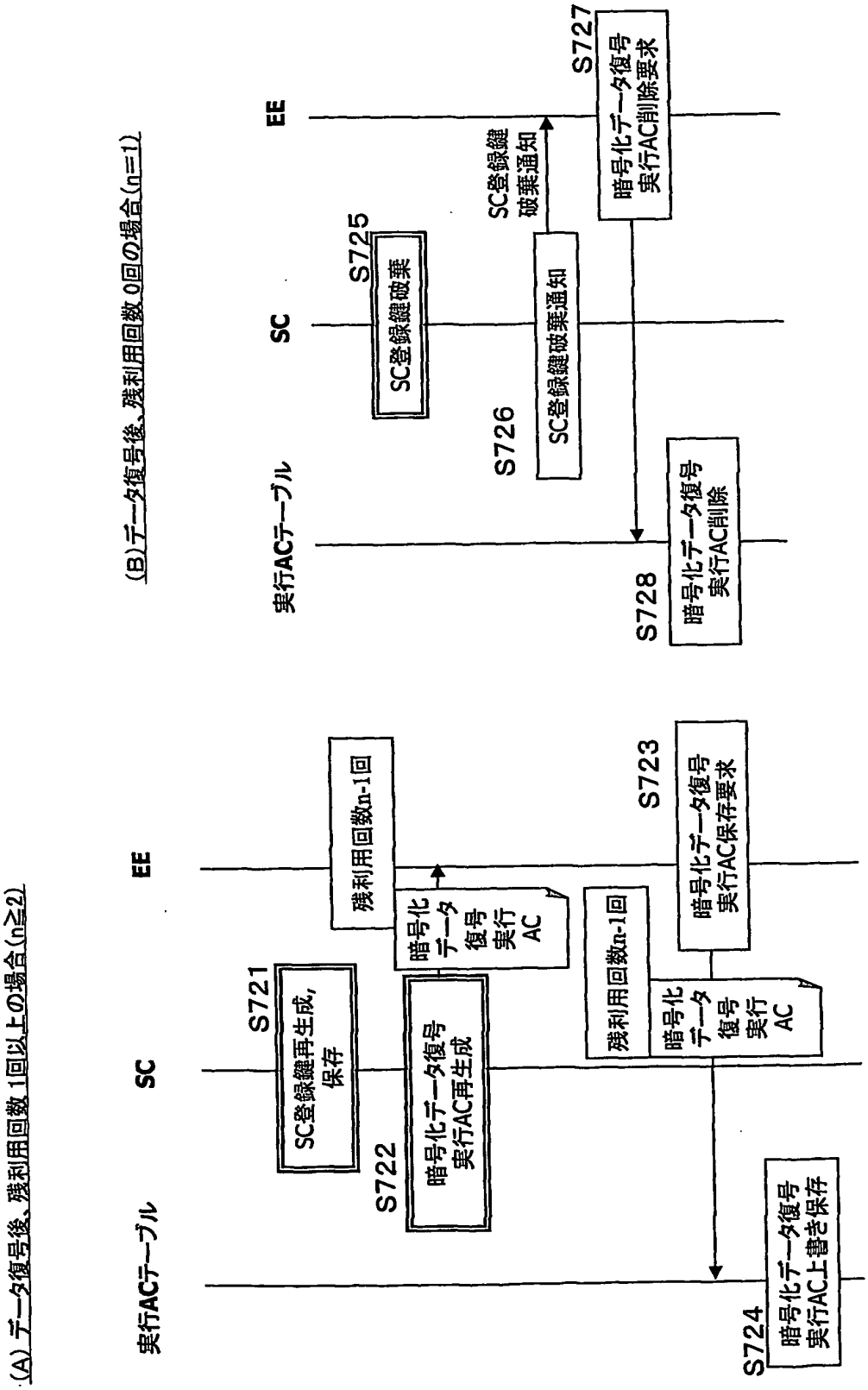

(A) データ復号後、残利用回数1回以上の場合(n≧2)
実行ACテーブル
SC
EE
S721
SC登録鍵再生成,保存
S722
暗号化データ復号実行AC再生成
残利用回数n-1回
暗号化データ復号実行AC
S723
暗号化データ復号実行AC保存要求
残利用回数n-1回
暗号化データ復号実行AC
S724
暗号化データ復号実行AC上書き保存
(B) データ復号後、残利用回数0回の場合(n=1)
実行ACテーブル
SC
EE
S725
SC登録鍵破棄
S726
SC登録鍵破棄通知
SC登録鍵破棄通知
S727
暗号化データ復号実行AC削除要求
S728
暗号化データ復号実行AC削除

Fig. 75

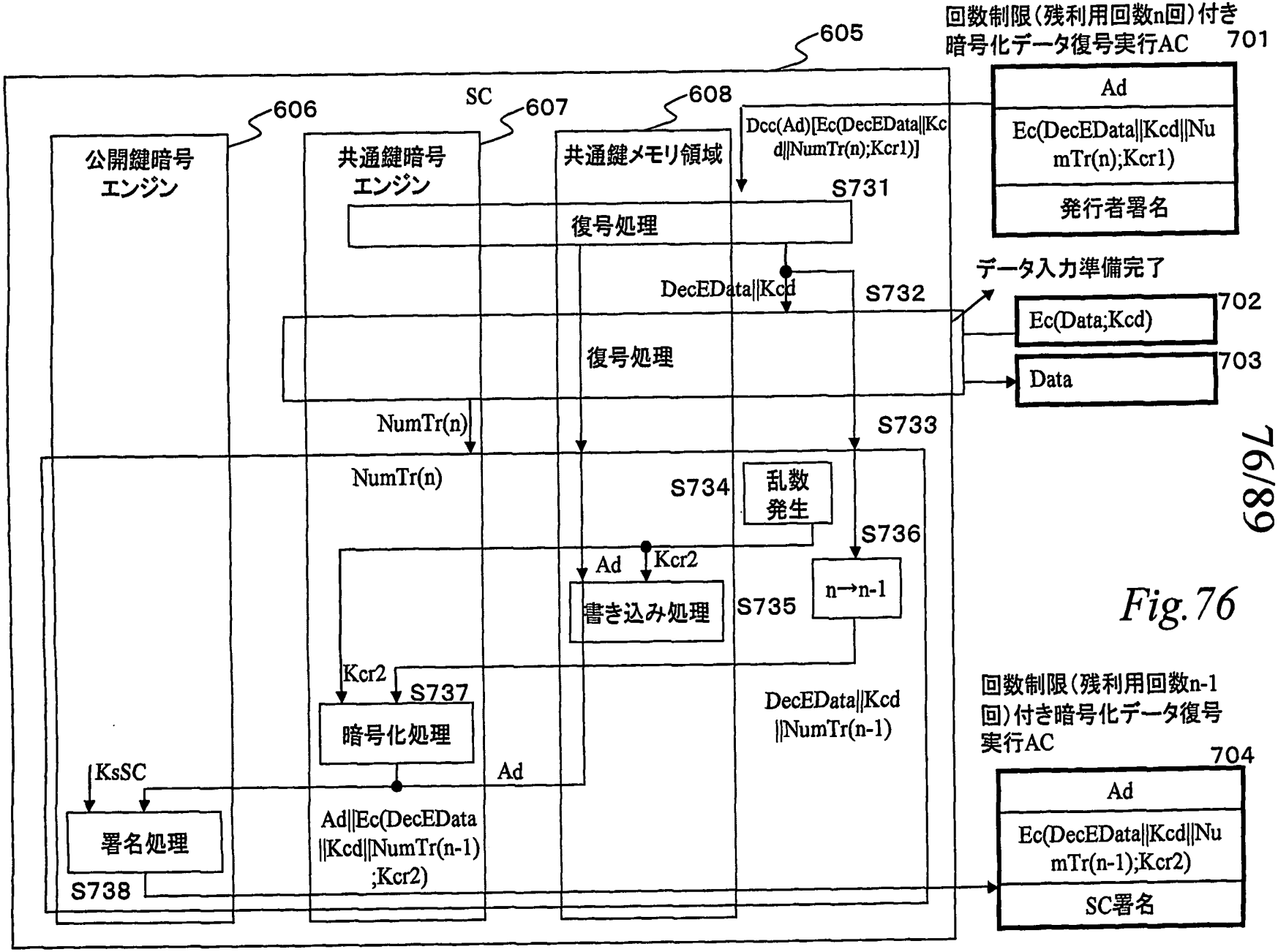

605
SC
606
607
608
公開鍵暗号
エンジン
共通鍵暗号
エンジン
共通鍵メモリ領域
Dcc(Ad)[Ec(DecEData||Kcd||NumTr(n);Kcr1)]
S731
復号処理
DecEData||Kcd
S732
復号処理
NumTr(n)
S733
NumTr(n)
S734
乱数
発生
S736
Ad
Kcr2
書き込み処理
S735
n→n-1
Kcr2
S737
暗号化処理
DecEData||Kcd
||NumTr(n-1)
KsSC
Ad
署名処理
Ad||Ec(DecEData
||Kcd||NumTr(n-1)
;Kcr2)
S738
回数制限(残利用回数n回)付き
暗号化データ復号実行AC
701
Ad
Ec(DecEData||Kcd||Nu
mTr(n);Kcr1)
発行者署名
データ入力準備完了
702
Ec(Data;Kcd)
703
Data
回数制限(残利用回数n-1
回)付き暗号化データ復号
実行AC
704
Ad
Ec(DecEData||Kcd||Nu
mTr(n-1);Kcr2)
SC署名

Fig. 76

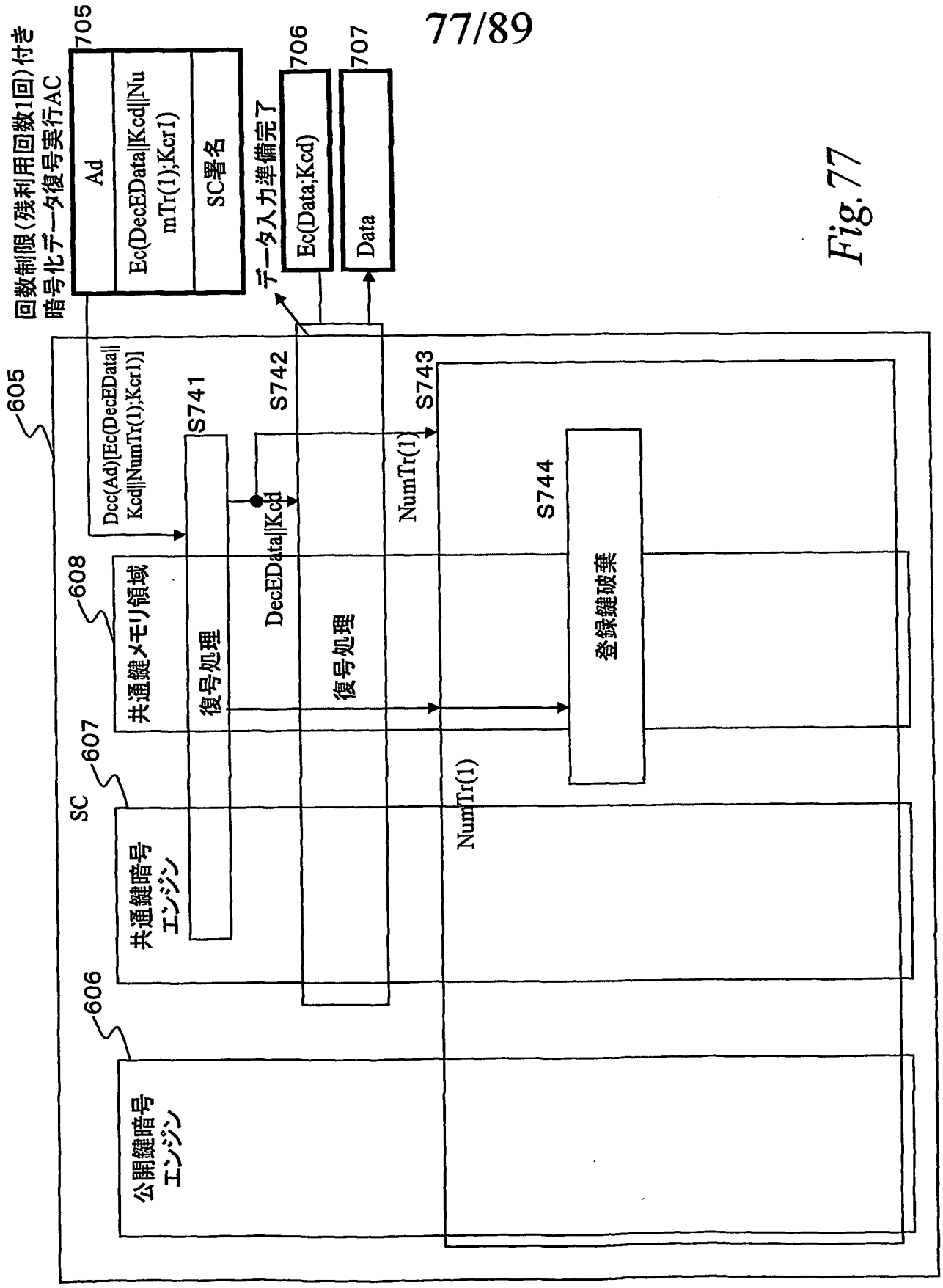

回数制限(残利用回数1回)付き
暗号化データ復号実行AC
705
Ad
Ec(DecEData||Kcd||Num Tr(1);Kcr1)
SC署名
706
707
データ入力準備完了
Ec(Data;Kcd)
Data
605
Dcc(Ad)[Ec(DecEData||Kcd||NumTr(1);Kcr1)]
S741
S742
S743
S744
608
共通鍵メモリ領域
復号処理
DecEData||Kcd
復号処理
NumTr(1)
登録鍵破棄
607
SC
共通鍵暗号エンジン
NumTr(1)
606
公開鍵暗号エンジン

Fig.77

Fig. 78

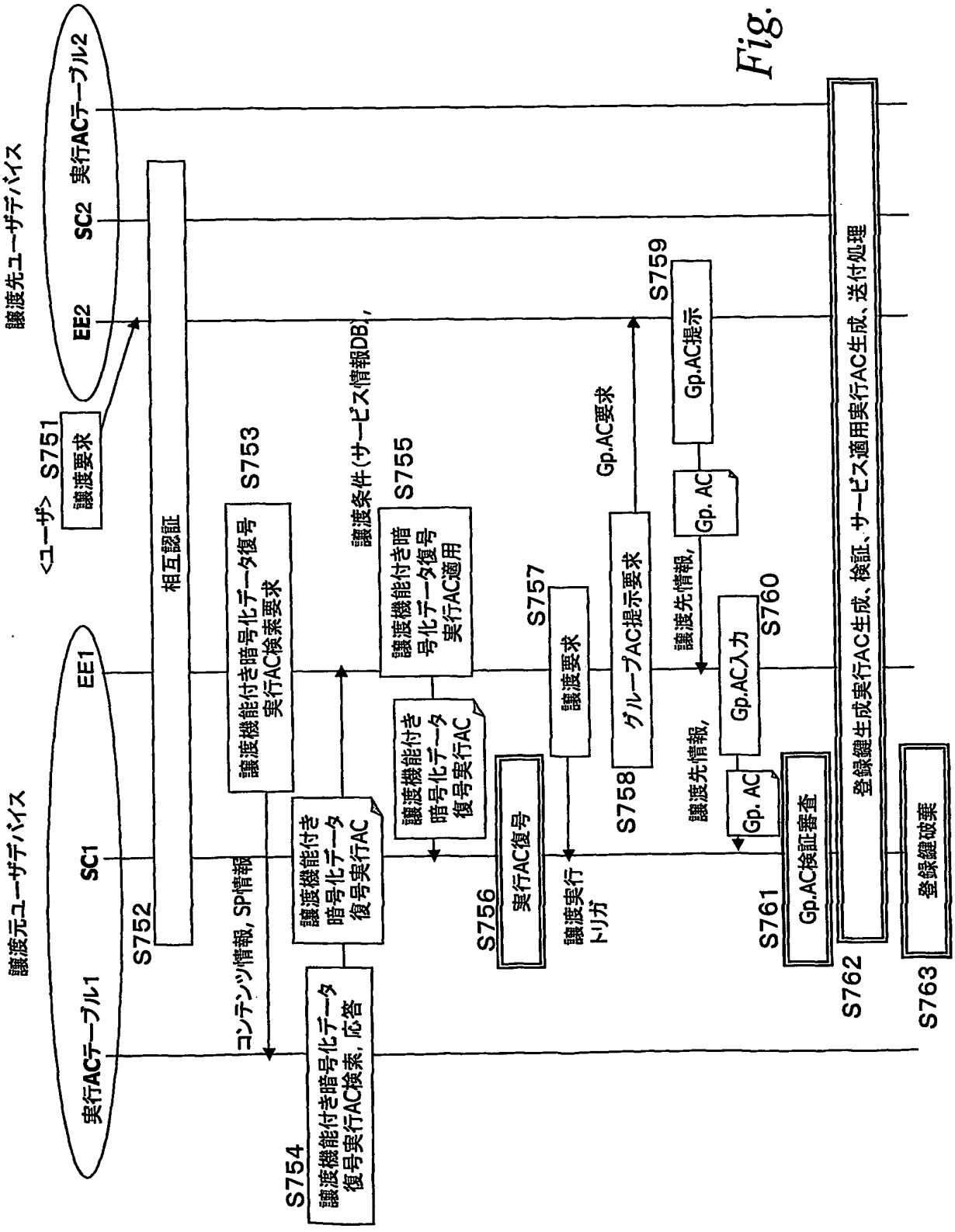

譲渡元ユーザデバイス
譲渡先ユーザデバイス
実行ACテーブル1
SC1
EE1
EE2
SC2
実行ACテーブル2
<ユーザ>
S751
譲渡要求
相互認証
S752
S753
譲渡機能付き暗号化データ復号
実行AC検索要求
コンテンツ情報, SP情報
S754
譲渡機能付き暗号化データ
復号実行AC検索, 応答
譲渡機能付き
暗号化データ
復号実行AC
譲渡条件(サービス情報DB),
S755
譲渡機能付き暗
号化データ復号
実行AC適用
譲渡機能付き
暗号化データ
復号実行AC
S756
実行AC復号
S757
譲渡要求
譲渡実行
トリガ
Gp.AC要求
S758
グループAC提示要求
S759
Gp.AC提示
Gp. AC
譲渡先情報,
譲渡先情報,
Gp. AC
S760
Gp.AC入力
S761
Gp.AC検証審査
S762
登録鍵生成実行AC生成、検証、サービス適用実行AC生成、送付処理
S763
登録鍵破棄

Fig.79

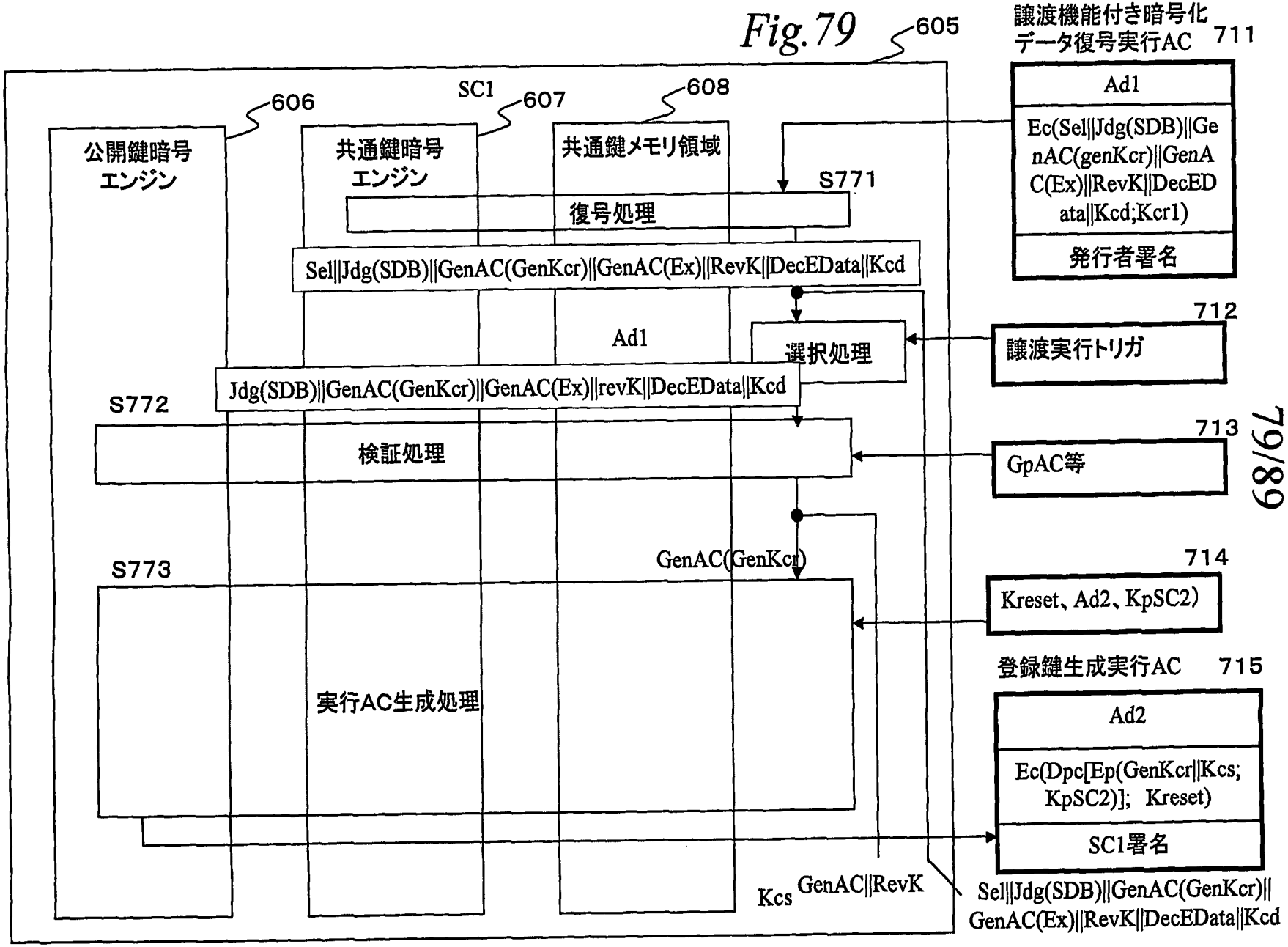
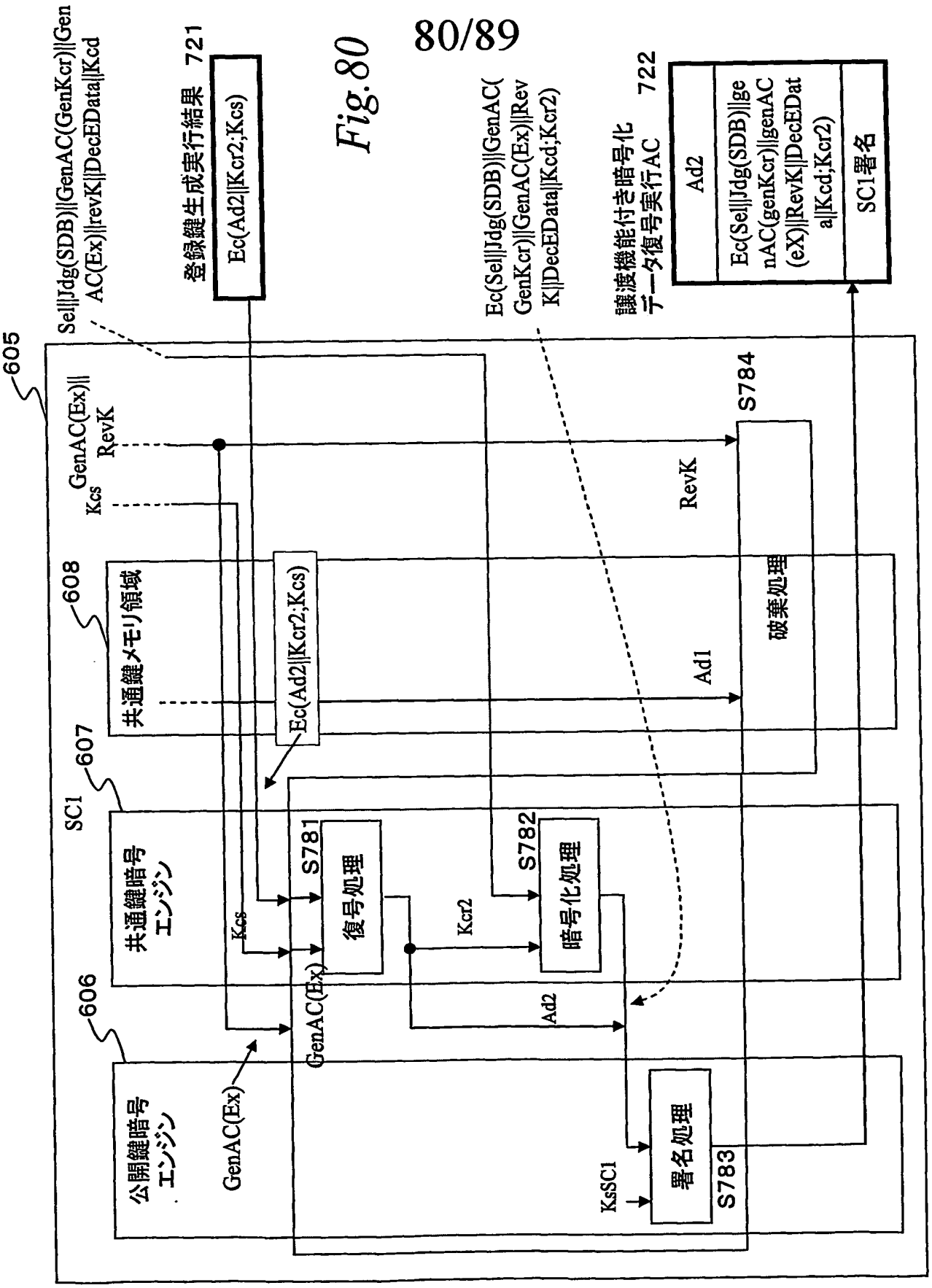

605
606
SC1
607
608
公開鍵暗号
エンジン
共通鍵暗号
エンジン
共通鍵メモリ領域
S771
復号処理
Sel||Jdg(SDB)||GenAC(GenKcr)||GenAC(Ex)||RevK||DecEData||Kcd
Ad1
選択処理
Jdg(SDB)||GenAC(GenKcr)||GenAC(Ex)||revK||DecEData||Kcd
S772
検証処理
S773
GenAC(GenKcr)
実行AC生成処理
Kcs
GenAC||RevK
譲渡機能付き暗号化
データ復号実行AC
711
Ad1
Ec(Sel||Jdg(SDB)||GenAC(genKcr)||GenAC(Ex)||RevK||DecEData||Kcd;Kcr1)
発行者署名
712
譲渡実行トリガ
713
GpAC等
714
Kreset、Ad2、KpSC2)
登録鍵生成実行AC
715
Ad2
Ec(Dpc[Ep(GenKcr||Kcs;KpSC2)]; Kreset)
SC1署名
Sel||Jdg(SDB)||GenAC(GenKcr)||GenAC(Ex)||RevK||DecEData||Kcd

Fig.80


605
606
607
608
721
722
SC1
公開鍵暗号エンジン
共通鍵暗号エンジン
共通鍵メモリ領域
登録鍵生成実行結果
Ec(Ad2||Kcr2;Kcs)
Sel||Jdg(SDB)||GenAC(GenKcr)||GenAC(Ex)||revK||DecEData||Kcd
GenAC(Ex)||RevK
Kcs
GenAC(Ex)
Ec(Ad2||Kcr2;Kcs)
S781
復号処理
Kcr2
S782
暗号化処理
Ad2
GenAC(Ex)
KsSC1
S783
署名処理
Ec(Sel||Jdg(SDB)||GenAC(GenKcr)||GenAC(Ex)||RevK||DecEData||Kcd;Kcr2)
譲渡機能付き暗号化データ復号実行AC
RevK
Ad1
S784
破棄処理
Ad2
Ec(Sel||Jdg(SDB)||genAC(genKcr)||genAC(eX)||RevK||DecEData||Kcd;Kcr2)
SC1署名

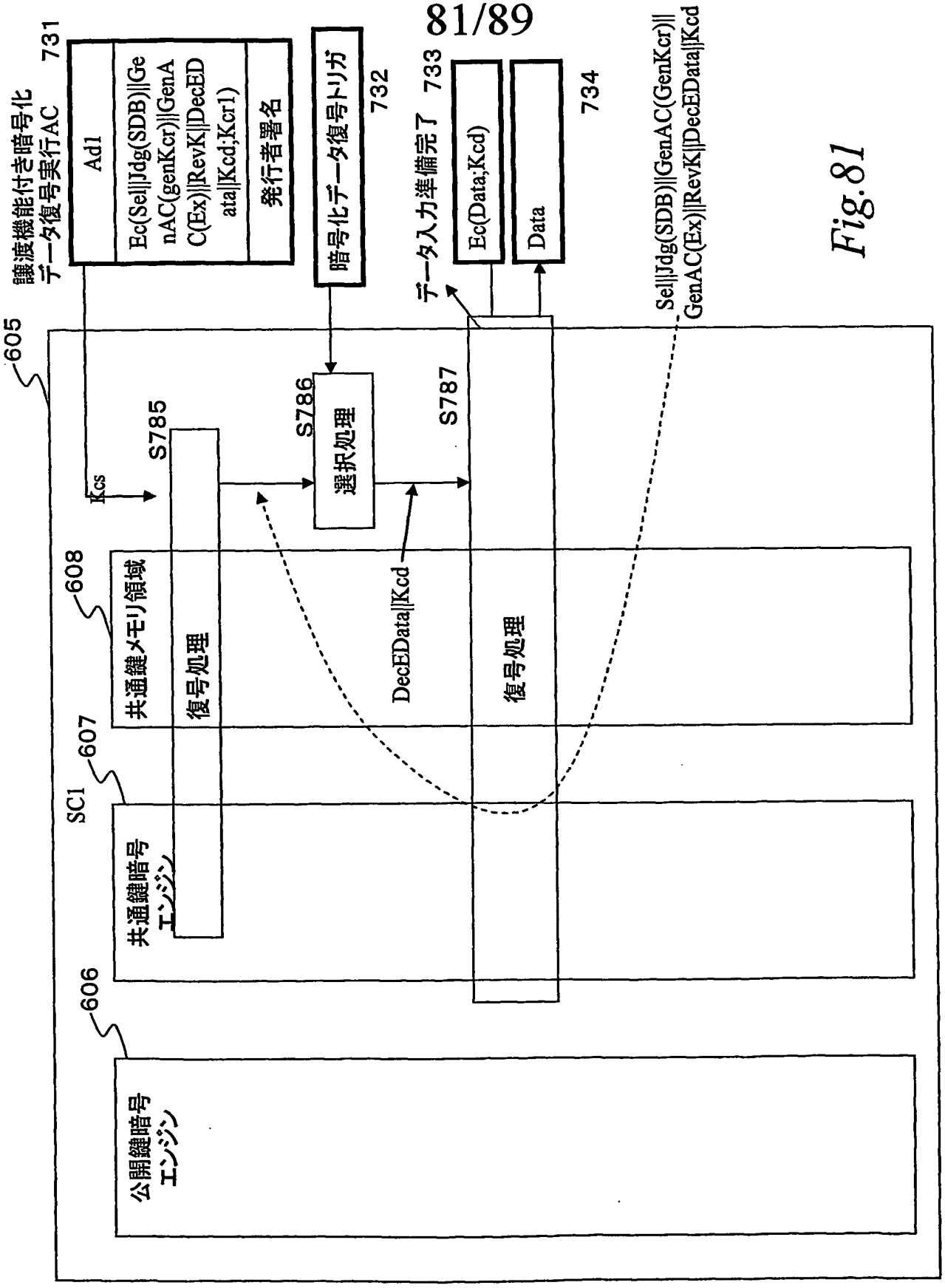
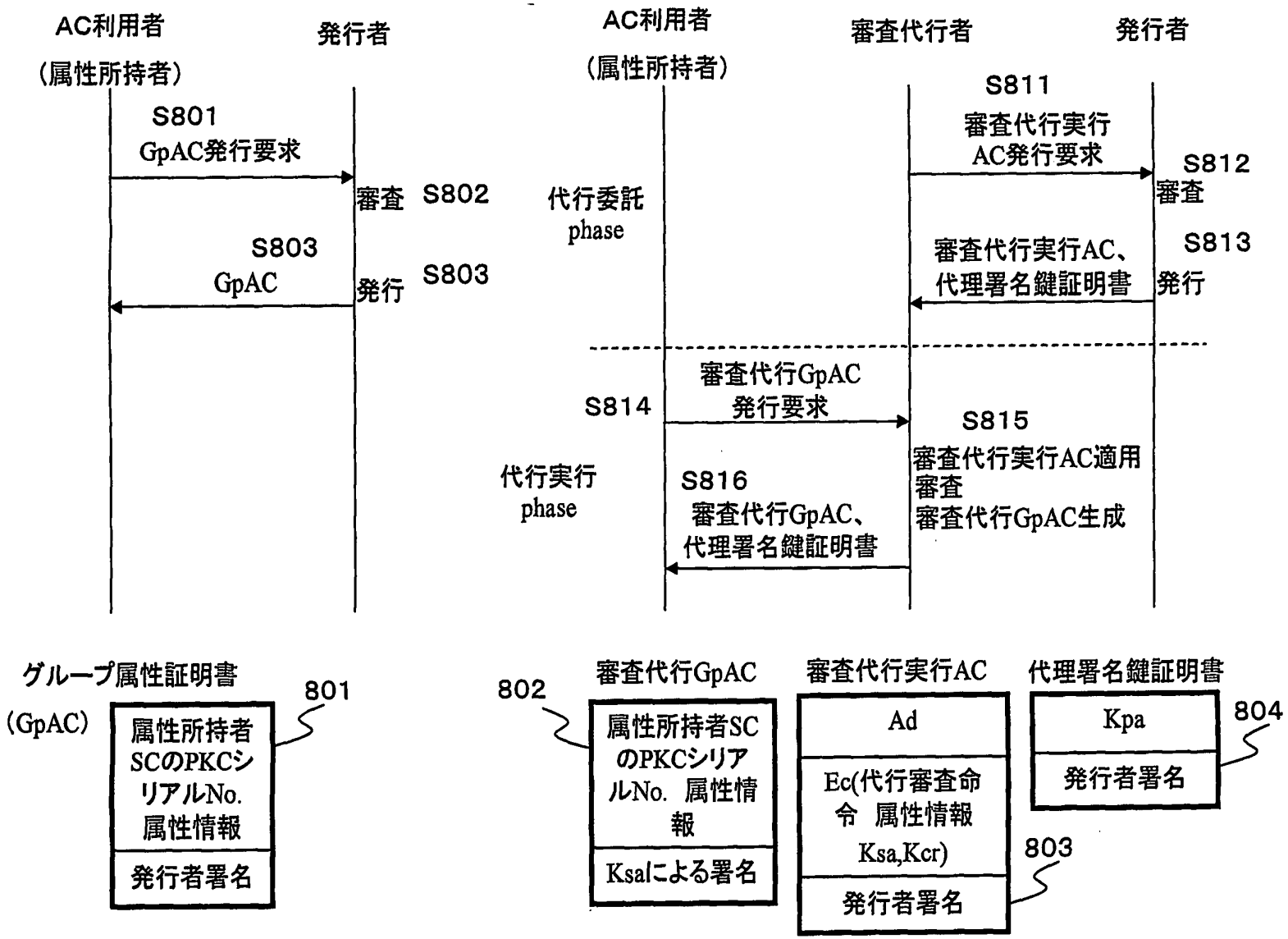

譲渡機能付き暗号化データ復号実行AC
731
Ad1
Ec(Sel||Jdg(SDB)||GenAC(genKcr)||GenAC(Ex)||RevK||DecEData||Kcd;Kcr1)
発行者署名
暗号化データ復号トリガ
732
データ入力準備完了
733
Ec(Data;Kcd)
Data
734
Sel||Jdg(SDB)||GenAC(GenKcr)||GenAC(Ex)||RevK||DecEData||Kcd
605
S785
S786
選択処理
S787
Kcs
608
共通鍵メモリ領域
復号処理
DecEData||Kcd
607
SC1
共通鍵暗号エンジン
復号処理
606
公開鍵暗号エンジン

Fig.81

Fig.82


(a)通常の属性証明書
(GpAC)発行構成
AC利用者
(属性所持者)
発行者
S801
GpAC発行要求
審査
S802
S803
GpAC
発行
S803
(b)審査代行実行属性証明書を適用
した属性証明書(GpAC)発行構成
AC利用者
(属性所持者)
審査代行者
発行者
S811
審査代行実行
AC発行要求
S812
審査
代行委託
phase
審査代行実行AC、
代理署名鍵証明書
S813
発行
審査代行GpAC
発行要求
S814
S815
審査代行実行AC適用
審査
審査代行GpAC生成
代行実行
phase
S816
審査代行GpAC、
代理署名鍵証明書
グループ属性証明書
(GpAC)
801
属性所持者
SCのPKCシ
リアルNo.
属性情報
発行者署名
802
審査代行GpAC
属性所持者SC
のPKCシリア
ルNo. 属性情
報
Ksaによる署名
審査代行実行AC
Ad
Ec(代行審査命
令 属性情報
Ksa,Kcr)
803
発行者署名
代理署名鍵証明書
Kpa
804
発行者署名

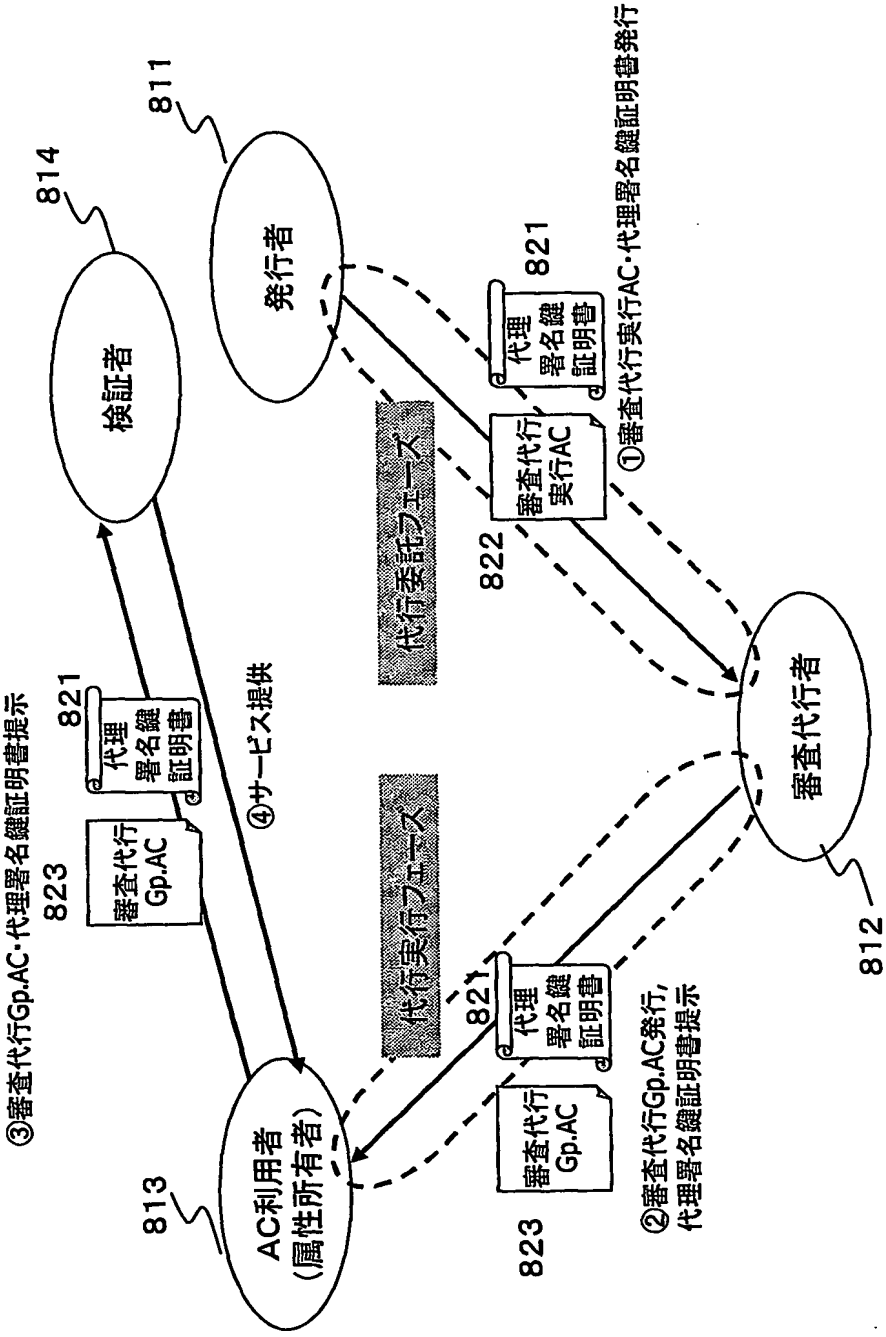

811
814
発行者
検証者
821
代理署名鍵証明書
審査代行実行AC
①審査代行実行AC・代理署名鍵証明書発行
822
代行委託フェース
③審査代行Gp.AC・代理署名鍵証明書提示
821
代理署名鍵証明書
審査代行Gp.AC
823
④サービス提供
代行実行フェース
審査代行者
812
821
代理署名鍵証明書
審査代行Gp.AC
823
②審査代行Gp.AC発行，代理署名鍵証明書提示
813
AC利用者（属性所有者）

Fig.83

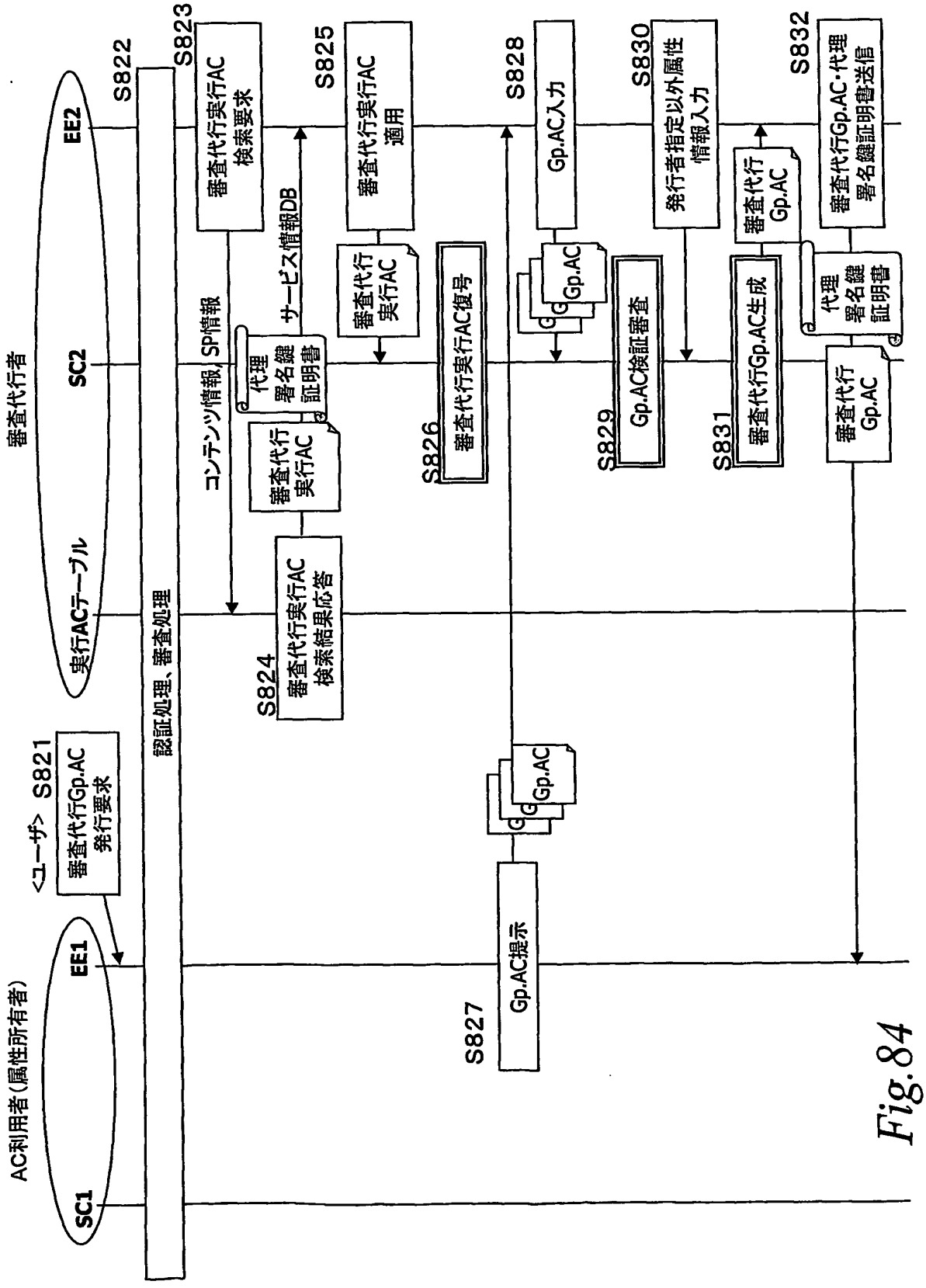

AC利用者(属性所有者)
審査代行者
EE1
EE2
SC1
SC2
実行ACテーブル
<ユーザ> S821
審査代行Gp.AC
発行要求
認証処理、審査処理
S822
S823
審査代行実行AC
検索要求
コンテンツ情報
SP情報
サービス情報DB
代理
署名鍵
証明書
審査代行
実行AC
S824
審査代行実行AC
検索結果応答
S825
審査代行実行AC
適用
審査代行
実行AC
S826
審査代行実行AC復号
S827
Gp.AC提示
Gp.AC
S828
Gp.AC入力
Gp.AC
S829
Gp.AC検証審査
S830
発行者指定以外属性
情報入力
S831
審査代行Gp.AC生成
S832
審査代行
Gp.AC
代理
署名鍵
証明書
審査代行Gp.AC・代理
署名鍵証明書送信
審査代行
Gp.AC

Fig. 84

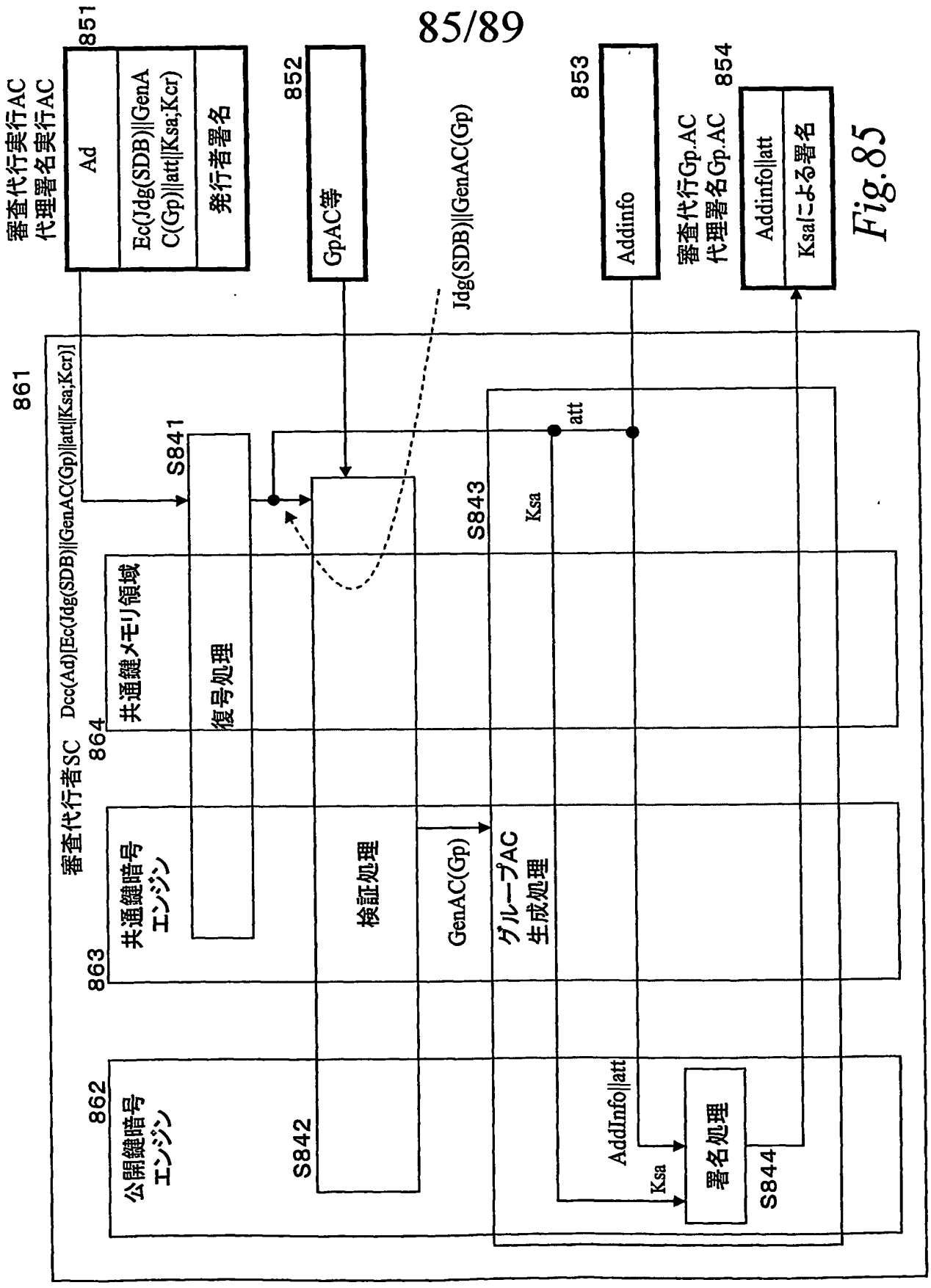

審査代行実行AC
代理署名実行AC
851
Ad
Ec(Jdg(SDB)||GenAC(Gp)||att||Ksa;Kcr)
発行者署名
852
GpAC等
853
Addinfo
審査代行Gp.AC
代理署名Gp.AC
854
Addinfo||att
Ksaによる署名
Jdg(SDB)||GenAC(Gp)
861
審査代行者SC
Dcc(Ad)[Ec(Jdg(SDB)||GenAC(Gp)||att||Ksa;Kcr)]
S841
復号処理
共通鍵メモリ領域
864
共通鍵暗号
エンジン
863
公開鍵暗号
エンジン
862
S842
検証処理
GenAC(Gp)
S843
Ksa
att
グループAC
生成処理
AddInfo||att
Ksa
署名処理
S844

Fig.85

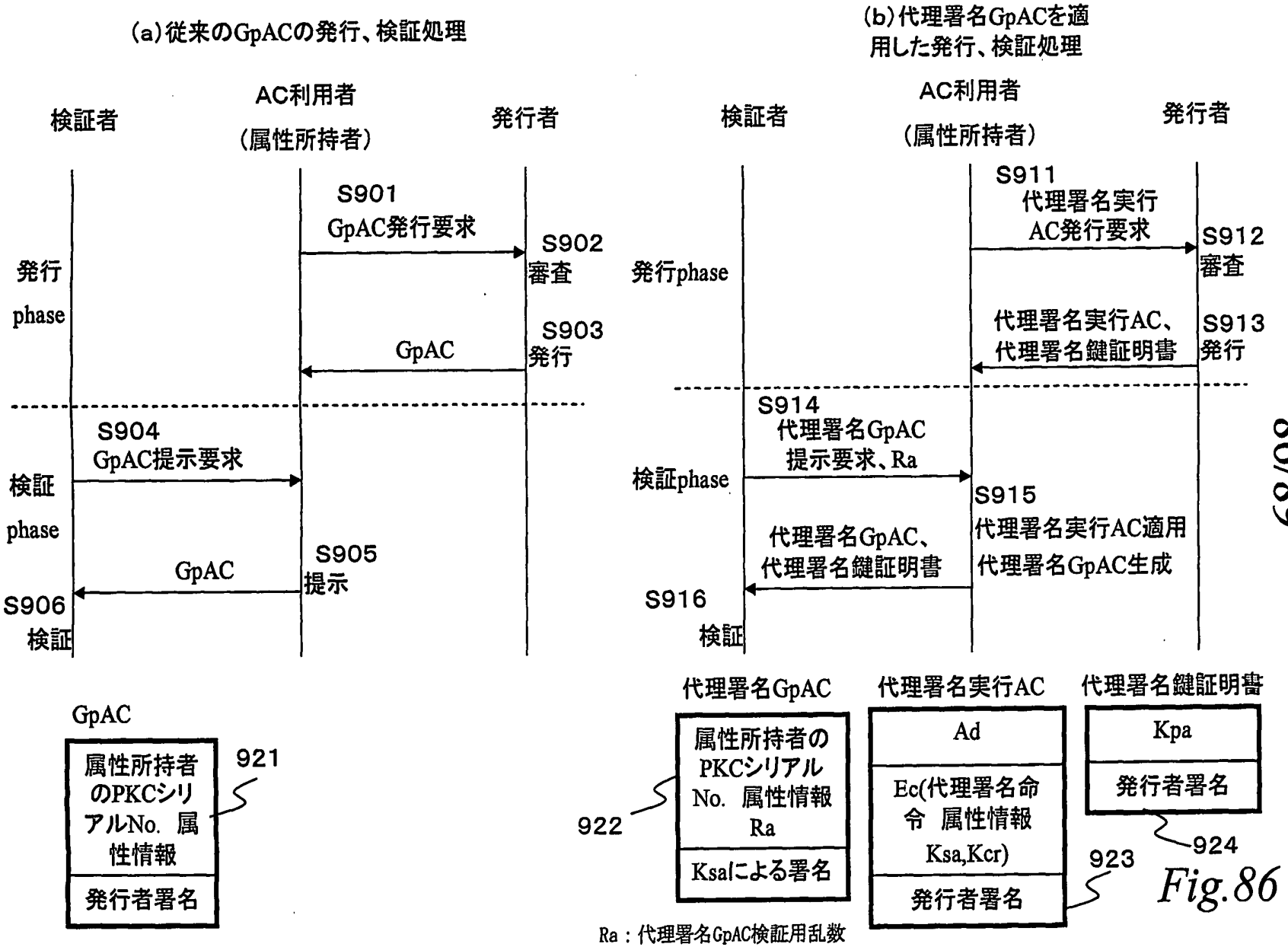

(a)従来のGpACの発行、検証処理
検証者
AC利用者
(属性所持者)
発行者
S901
GpAC発行要求
S902
審査
発行
phase
S903
発行
GpAC
S904
GpAC提示要求
検証
phase
S905
提示
GpAC
S906
検証
GpAC
属性所持者のPKCシリアルNo. 属性情報
921
発行者署名
(b)代理署名GpACを適用した発行、検証処理
検証者
AC利用者
(属性所持者)
発行者
S911
代理署名実行AC発行要求
S912
審査
発行phase
代理署名実行AC、代理署名鍵証明書
S913
発行
S914
代理署名GpAC提示要求、Ra
検証phase
S915
代理署名実行AC適用
代理署名GpAC生成
代理署名GpAC、代理署名鍵証明書
S916
検証
代理署名GpAC
属性所持者のPKCシリアルNo. 属性情報 Ra
922
Ksaによる署名
代理署名実行AC
Ad
Ec(代理署名命令 属性情報 Ksa,Kcr)
923
発行者署名
代理署名鍵証明書
Kpa
発行者署名
924
Ra：代理署名GpAC検証用乱数

Fig.86

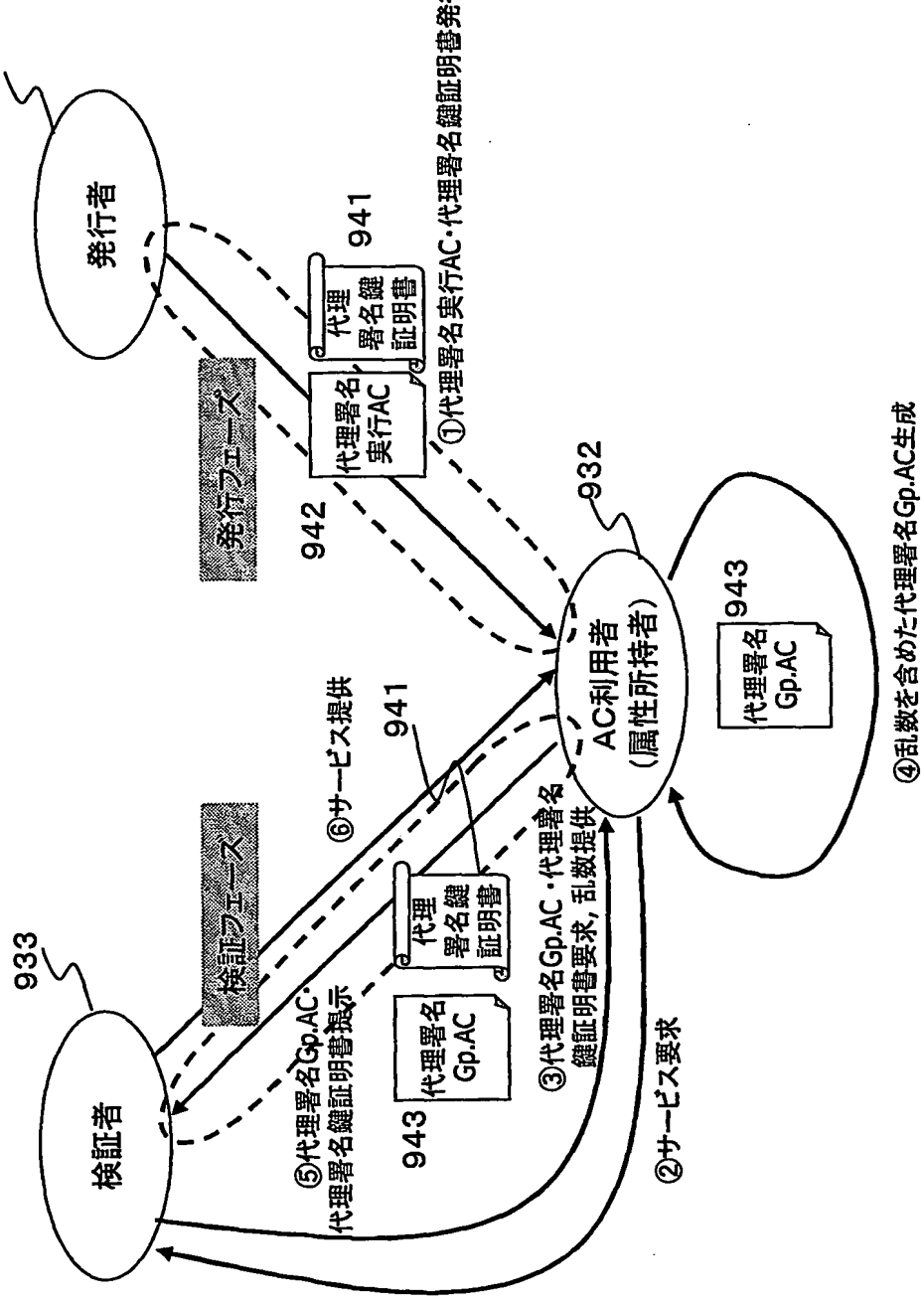

931
発行者
941
代理署名鍵証明書
代理署名実行AC
①代理署名実行AC・代理署名鍵証明書発行
発行フェーズ
942
932
AC利用者
(属性所持者)
943
代理署名Gp.AC
④乱数を含めた代理署名Gp.AC生成
⑥サービス提供
941
検証フェーズ
933
検証者
⑤代理署名Gp.AC・
代理署名鍵証明書提示
代理署名鍵証明書
943
代理署名Gp.AC
③代理署名Gp.AC・代理署名
鍵証明書要求, 乱数提供
②サービス要求

Fig.87

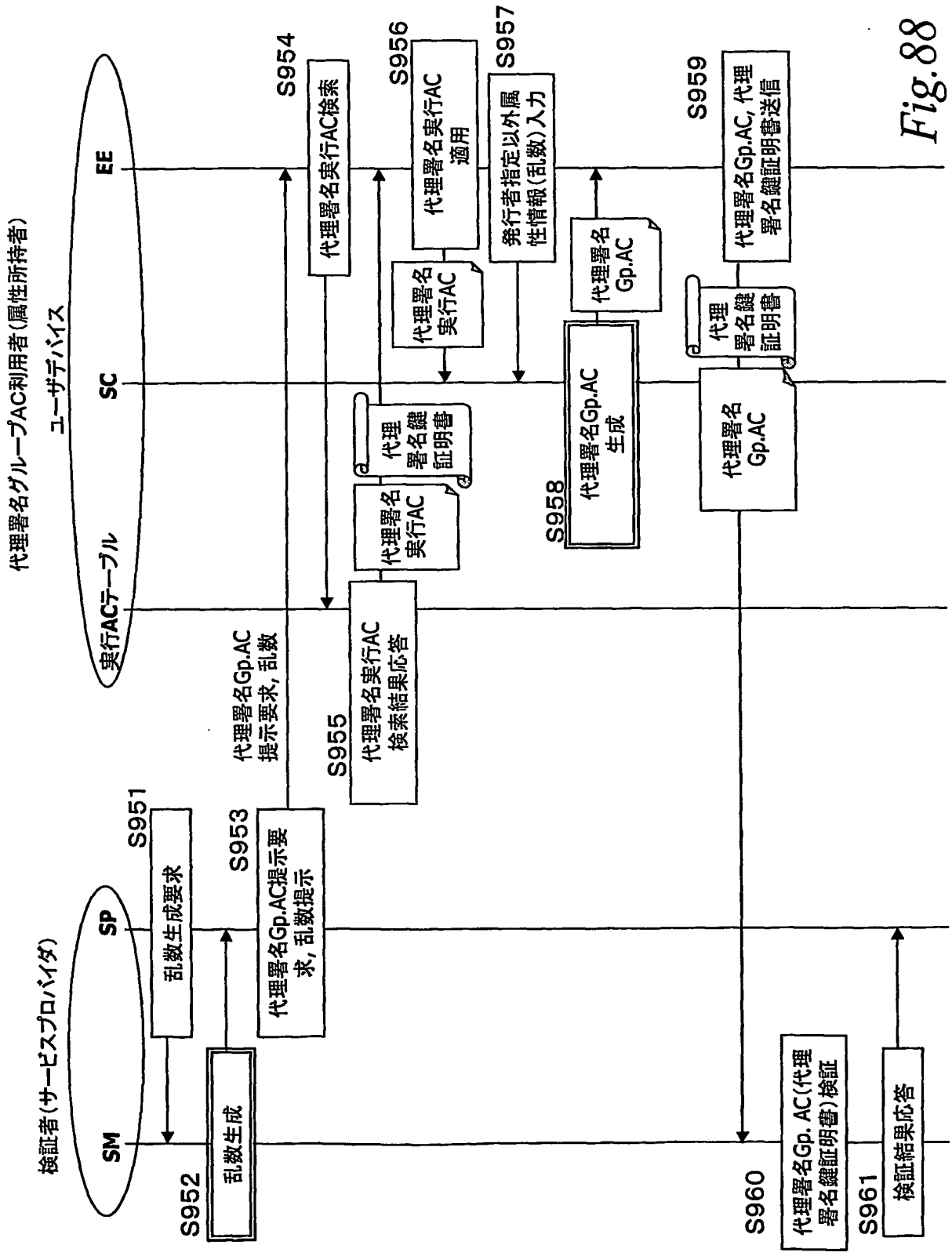

代理署名グループAC利用者(属性所持者)
ユーザデバイス
検証者(サービスプロバイダ)
SM
SP
SC
EE
実行ACテーブル
S951
乱数生成要求
S952
乱数生成
S953
代理署名Gp.AC提示要求, 乱数提示
S954
代理署名実行AC検索
S955
代理署名実行AC検索結果応答
S956
代理署名実行AC適用
S957
発行者指定以外属性情報(乱数)入力
S958
代理署名Gp.AC生成
S959
代理署名Gp.AC, 代理署名鍵証明書送信
S960
代理署名Gp. AC(代理署名鍵証明書)検証
S961
検証結果応答
代理署名Gp.AC提示要求, 乱数
代理署名実行AC
代理署名鍵証明書
代理署名Gp.AC
代理署名実行AC
代理署名鍵証明書
代理署名Gp.AC

Fig. 88

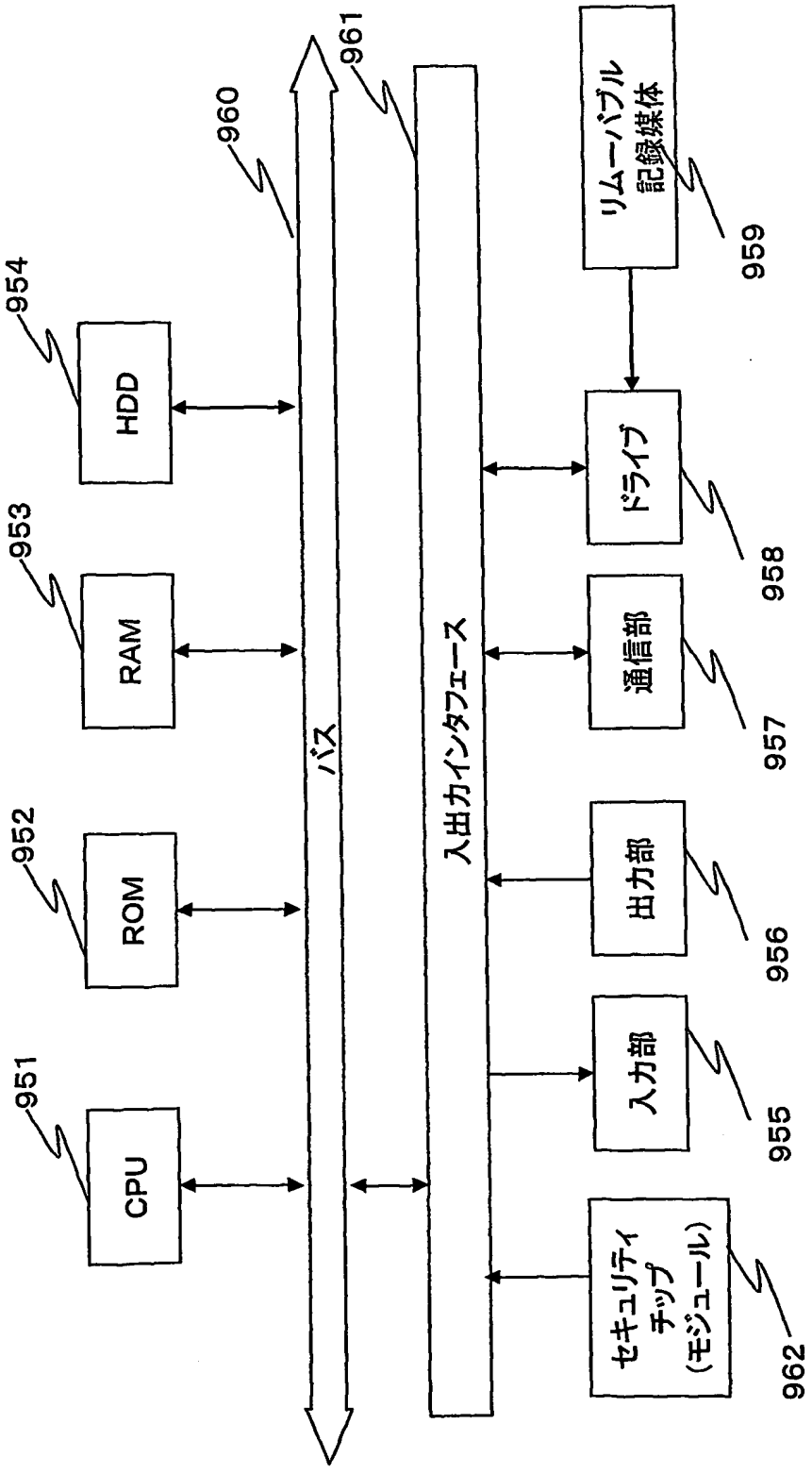

CPU
951
ROM
952
RAM
953
HDD
954
バス
960
961
入出力インタフェース
リムーバブル記録媒体
959
ドライブ
958
通信部
957
出力部
956
入力部
955
セキュリティチップ(モジュール)
962

Fig.89

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/JP03/06585

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, G06F17/60, G06F15/00, G06F12/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, certificate, attribute

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-139998 A (Sony Corp.), 17 May, 2002 (17.05.02), Par. Nos. [0337] to [0424] (Family: none)	1-4,7-11, 13-16,19-21, 23-25,30-32, 34,36-38, 43-45,47-50, 62,63,72,74, 75
Y		5,6,12,17, 18,22,26-29, 33,35,39-42, 46,51-55,60, 61,64-68,73
A		56-59,69-71

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 12 September, 2003 (12.09.03)	Date of mailing of the international search report 30 September, 2003 (30.09.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/JP03/06585

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Yasutsugu KAWAKURA, "ID Shomeisho to Zokusei Shomeisho no Heiyo ni yoru Access Seigyo Hoshiki", Computer Security Symposium' 98 Ronbunshu", pages 97 to 102, 29 October, 1998 (29.10.98), Shomei Kikan to Shomeisho oyobi 3.2.4 Shomeisho no Keishiki	5,6,12,17, 18,22,28,29, 35,41,42,51, 54,60,64,67, 73
Y	JP 2001-67319 A (Hitachi, Ltd.), 16 March, 2001 (16.03.01), Par. Nos. [0019] to [0022] (Family: none)	6,18
Y	JP 8-160856 A (Nippon Telegraph And Telephone Corp.), 21 June, 1996 (21.06.96), Par. Nos. [0017] to [0052] & EP 715242 B1 & US 5701343 A & DE 69529801 T2	26,33,39,46, 55,68
Y	WO 01/023980 A1 (HEWLETT-PACKARD CO.), 05 April, 2001 (05.04.01), Page 10, line 30 to page 11, line 4; page 35, line 24 to page 38, line 17 & JP 2003-510713 A & EP 1224516 A1	27,40,53,57, 61,66,70
Y	Todd Sundsted, "Peer to Peer·Computing no Jissen: Peer to Peer·Network ni okeru Shinraisei to Security", [online], 14 December, 2001 (14.12.01), [retrieval date 11 September, 2003 (11.09.03)], Internet <URL:http://www-6.ibm.com/jp/developerworks/java/library01.html>, Secur·System no Element oyobi Security no Jissen	52,65

国際調査報告

国際出願番号　PCT／JP03／06585

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／32, G06F17／60, G06F15／00, G06F12／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2003年
日本国登録実用新案公報	1994－2003年
日本国実用新案登録公報	1996－2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル（JOIS），WPI
certificate, attribute

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2002-139998 A（ソニー株式会社） 2002.05.17, 第337-424段落（ファミリなし）	1-4, 7-11, 13-16, 19-21, 23-25, 30-32, 34, 36-38, 43-45, 47-50, 62, 63, 72, 74, 75

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 12. 09. 03	国際調査報告の発送日 30.09.03
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里　裕正　5M　9364 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y		5, 6, 12, 17, 18, 22, 26-29, 33, 35, 39-42, 46, 51-55, 60, 61, 64-68, 73
A		56-59, 69-71
Y	川倉康嗣，ＩＤ証明書と属性証明書の併用によるアクセス制御方式，コンピュータセキュリティシンポジウム’９８論文集，p. 97-102, 1998. 10. 29, 3. 2. 2 証明機関と証明書 及び 3. 2. 4 証明書の形式	5, 6, 12, 17, 18, 22, 28, 29, 35, 41, 42, 51, 54, 60, 64, 67, 73
Y	JP 2001-67319 A（株式会社日立製作所）2001. 03. 16, 第19-22段落（ファミリなし）	6, 18
Y	JP 8-160856 A（日本電信電話株式会社）1996. 06. 21, 第17-52段落 & EP 715242 B1 & US 5701343 A & DE 69529801 T2	26, 33, 39, 46, 55, 68
Y	WO 01/023980 A1 (HEWLETT-PACKARD COMPANY) 2001. 04. 05, 第10頁第30行～第11頁第4行，第35頁第24行～第38頁第17行 & JP 2003-510713 A & EP 1224516 A1	27, 40, 53, 57, 61, 66, 70
Y	Todd Sundsted, ピアツーピア・コンピューティングの実践：ピアツーピア・ネットワークにおける信頼性とセキュリティー，[online], 2001. 12. 14, [検索日 2003. 09. 11], インターネット <URL:http://www-6. ibm. com/jp/developerworks/java/library01. html>, セキュア・システムのエレメント 及び セキュリティーの実践	52, 65